ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҰЙЫМДАРДЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ ЖҮЙЕСІНІҢ АУДИТІ

Информационная технология
АУДИТ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

ҚР СТ 34.030 - 2008

Ресми басылым

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

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҰЙЫМДАРДЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ ЖҮЙЕСІНІҢ АУДИТІ

ҚР СТ 34.030 - 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 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

Кіріспе

Осы стандарт негізінен ақпараттық қауіпсіздік бойынша мамандар сияқты ақпараттық қауіпсіздікті енгізуге жауапты ұйым қызметкерлеріне, сондай-ақ ҚР СТ ИСО/МЭК 27001-2008 енгізілген басқару құралдарын бағалаумен айналысатын тұлғалар үшін, мысалы, осы стандартқа сәйкестік деңгейін тексеру үшін немесе ішкі аудит мақсатына бейімделген. Жетекшілік сондай-ақ ақпараттық қауіпсіздікті басқару жүйелерін (АҚБЖ) күйге келтіру барысында әзірлеушілер үшін және бағалау жүргізетін ішкі аудиторлар үшін пайдалы бола алады.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҰЙЫМДАРДЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ ЖҮЙЕСІНІҢ АУДИТІ

Енгізілген күні 2008.07.01.

1 Қолданылу саласы

Осы стандарт олардың ақпараттық қауіпсіздікті басқару жүйесі (АҚБЖ) ҚР СТ ИСО/МЭК 27001:2008 стандартына сәйкесетіндігін өздері тексергісі келетін ұйымдарда пайдалануға арналған және ҚР СТ ИСО/МЭК 27001 стандартына сәйкестікке сертификатталуға дайындыққа ұйымдарға көмекке әзірленген. Сәйкестікке арналған тексерулерді ақпараттық қауіпсіздікке жауапты ұйым қызметкерінің бақылауымен немесе меншікті аудиторлар күшімен жүргізу ұсынылады.

Осы стандарттың мақсаты – ұйымдарға өздерінің АҚБЖ *ИСО/МЭК 27001* стандартының талаптарына сәйкестігі дәрежесін бағалауға мүмкіндік беру. Осы стандартта стандартқа сәйкестікті тексеруге дайындалу және орындау бойынша ақпарат келтірілген. Стандартқа сәйкестікті тексерудің өзі негізінен сауалнаманы толтыру болып табылады.

Нақты тексеру осы стандарттың 5 және 5 бөлімдерінде келтірілген:

– 5-бөлім *ҚР СТ ИСО/МЭК 27001* стандартының талаптарын орындауды бағалау – аталмыш сауалнама ақпараттық қауіпсіздік саласындағы ұйымның күйі сәйкестігін тексеруге рұқсат береді.

– 6-бөлім ИСО/МЭК 27001 стандартымен қарастырылған басқару құралдарының және мақсаттарының аудиты.

Осы стандарт АҚБЖ талаптарға сәйкестігіне қол жеткізу мақсатында АҚБЖ процестерін тексеру үшін жұмыс кітабын пайдаланумен АҚБЖ-ң *ҚР СТ ИСО/МЭК 27001* стандартының талаптарына сәйкестігін тексеруді жүргізуіне ұйымдарға көмек тәсілі болып табылады.

Сәйкессіздікті талдау *ҚР СТ ИСО/МЭК 27001* стандартының талаптарына басқару құралдарының сәйкес келетіндігін растау құралы ретінде ғана қызмет етеді. Егер кейбір құралдар стандартқа толық сәйкес келмесе, ұйым сәйкессіздік себептерін құжаттауы тиіс. *ҚР СТ ИСО/МЭК 27001* стандартына сәйкестікті бағалауды жүргізе алатын аудиторлар басқалай заттардан бөлек осы себептерге және олардың негіздемесіне күдіктенуге қабілетті болуы тиіс. Осы стандарттың ақпараттық құрал ретінде қызмет ететіндігін және *ҚР СТ ИСО/МЭК 27001* стандартына сәйкестік шараларын анықтаудың құралы болып табылмайтындығын атап өту қажет.

Ұйымдар сәйкессіздік талдауын, мысалы, тапсырыс берушімен орындалатын репетициялық аудитті немесе АҚБЖ ішкі аудитын жүргізудің алдында *ҚР СТ ИСО/МЭК 27001* стандартына сәйкестікті бейресми бағалау үшін пайдалана алады. Сәйкессіздік талдауы аккредиттелген мамандармен жүргізілетін сертификаттау үшін формальды мағынаға ие емес және қолдану туралы бекітілген ережелерді қалыптастыру кезінде пайдаланыла алмайды, өйткені ол қолдану туралы ережеге қойылатын *ҚР СТ ИСО/МЭК 27001* стандартымен бекітілген талаптарға сәйкес келмейді.

АҚБЖ процестерін тексеру ұйымда *ҚР СТ ИСО/МЭК 27001* стандартымен анықталған талаптарды орындау үшін қажетті тиісті жүйелер және процестердің барлығын растау құралы ретінде қызмет етеді. Бұл тексеру аккредиттелген мамандармен жүргізілетін сертификаттауға дайындалушы ұйымдармен, сонымен қатар бақылау аудиты секілді сертификаттаудан кейін орындалатын операцияларға және қайталама сертификаттауға дайындалушылармен орындалуы тиіс. Ол қанша операциялардың орындалғандығын және әлі қаншалықты орындалуға тиістігін тексеруге рұқсат беретін құрал болып табылады. Бұл тексеру операциялардың қаншалықты жақсы және тиімді болғандығын немесе бақылау жүйесінің қаншалықты дұрыс және тиімді ұйымдастырылғандығын көрсетпейді.

Осы стандарт *ҚР СТ ИСО/МЭК 27001* стандартында қамтылған АҚБЖ процестерін енгізу және аудиты бойынша мәселелерді қарастырмайтындығын атап өту маңызды.

2 Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтемелер пайдаланылды:

ҚР СТ 1.9-2003 Қазақстан Республикасының мемлекеттік стандарттау жүйесі. Халықаралық, өңірлік және ұлттық стандарттарды және стандарттау, метрология, сертификаттау және аккредиттеу жөніндегі нормативтік құжаттарды қолдану тәртібі.

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

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

ҚР СТ 34.028-2008 Ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерін сараптау, бағалау және сертификаттау тәртібі;

ҚР СТ 34.029-2008 Ақпараттық технология. Бағалау және тәуекелдерді басқару.

ИСО/МЭК 62; 1996 жетекшілігі Сапа жүйелерінің сертификатталуын жүргізетін сертификаттау жөніндегі органдарға қойылатын жалпы талаптар.

ИСО/МЭК 73:2002 жетекшілігі Тәуекелдерді басқару. Терминология. Стандарттарда пайдалану бойынша нұсқаулық.

ЕА 7/03 ақпараттық қауіпсіздікті басқару жүйелерін тіркеу/сертификаттау жөніндегі органдарды аккредиттеу үшін нұсқаулық.

Ескертпе – Көрсетілген стандарттардың дұрыс нұсқасы пайдаланылуы керек.

3 Терминдер мен анықтамалар

Осы стандартта ИСО/МЭК 73:2002 Нұсқаулығында келтірілген терминдер пайдаланылады.

4 АҚБЖ қолданылу саласы

АҚБЖ қолданылу саласы АҚБЖ стандартқа сәйкестігін тексеретін ұйым үшін де, сондай-ақ аудиторлар үшін де екіұшты анықталмауы және анық болуы өте маңызды.

Көптеген бизнес-қосымшалардың және процестердің және ақпараттық жүйелердің, технологиялардың және желілердің дамуының өмір сүретін күрделілігінде АҚБЖ қолданылу саласын белгілеудің көптеген тәсілдері бар. Осындай түрде, ұйымның өлшемі және оның территориалдық бытыраңқылығы АҚБЖ қолданудың балама саласы жөніндегі түсінікке әсер етеді. Іскерлік қолдануларға арналған жүйелер автономды түрде өте сирек жағдайларда жұмыс істейді, өйткені олар басқа жүйелермен өзара әрекеттесуі тиіс. Осылайша, АҚБЖ қолдану аясын анықтау кезінде аталмыш АҚБЖ шегіндегі процестермен және басқа жүйелермен барлық байланыстарды назарға алу қажет.

АҚБЖ қолдану салаларын айқындау және анықтау бойынша нұсқаулар осы стандартта беріледі, онда *ҚР СТ ИСО/МЭК 27001* стандартында келтірілген анықтама толығырақ түсіндіріледі. Стандартта АҚБЖ қолданылу саласы ұйым терминдерінде, оның орналасқан жерінде, ресурстарында және технологиясында сипатталады. Неғұрлым толық түсіну үшін мұнда ақпараттық ресурстарды, бизнес-ұсыныстарды және процестерді, сонымен қатар пайдаланылатын технологияны қосу қажет. Бұл элементтерді ұсақ-түйегіне дейін анықтаудың қажеттілігі жоқ болса да, барлық елеулі ресурстарды айқындау маңызды.

5 *ҚР СТ ИСО/МЭК* 27001 стандарты талаптарының орындауын бағалау

Келесі берілген 1-кесте *ҚР СТ ИСО/МЭК 27001* стандартының негізгі бөлімінің нормаларын орындау бағаларын алу үшін арналған. Егер Ішінара немесе Жоқ жолындағы ұяшықтардың бірі белгімен белгіленсе, 1-кестенің

төменде келтірілген ұяшықтарында себептерін және негіздемесін көрсету қажет.

2-кесте ИСО/МЭК 27001 стандартының А қосымшасы талаптарының орындалуына бағалау алу үшін арналған.

1-Кесте – ИСО/МЭК 27001:2005 стандарты бөлімдерінің талаптарына сәйкестікті бағалау

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
4.2 АҚБЖ құру және басқару				
4.2.1 АҚБЖ құру ***Ұйым:***				
а) Бизнес, ұйым, орналасқан жер, активтер және технологиялар сипаттамаларының терминдерінде АҚБЖ қолдану аясын және шекарасын анықтау, бұл жағдайда қолдану аясынан барлық ерекше жағдайлар үшін толық негіздеме келтіруі тиіс ***(ИСО/МЭК 27001:2005, 1.2 қараңыз)***				
4.2.1.a.1 АҚБЖ қолданылу саласын және шекарасын бір мәнде анықтайтын құжат бар ма?				
4.2.1.a.2 Көрсетілген анықтама бизнестің, ұйымның, оның орналасқан жерінің, активтер және технологиялардың сипаттамалары жөнінде ақпаратты қамтиды ма?				
4.2.1.a.3 Қолданылу саласындағы елеулі ерекше жағдайлар сәйкестендірілді ме және көрсетілген ерекше жағдайлардың анық түсіндірмесі және негіздемесі берілді ме?				
b) Б*изнестің, ұйымның, оның орналасқан жерінің, активтер және технологиялардың сипаттамаларының* ***терминдерінде АҚБЖ саясатын анықтауға тиісті.***				
4.2.1.b.1 Берілген АҚБЖ қолдану аясын қамтитын АҚБЖ саясаты анықталды ма?				
4.2.1.b.2 Көрсетілген саясат мақсаттарды анықтау үшін жалпы				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
құрылымды қамтиды ма және ол ақпараттық қауіпсіздікке қатысты қызмет ұстанымдарын және нұсқаулықтың жалпы міндеттерін береді ме?				
4.2.1.b.3 Бұл саясат өндірістік және құқықтық немесе нормативтік талаптарды, сонымен қатар қауіпсіздік бойынша шарттық міндеттемелерді ескереді ме?				
4.2.1.b.4 Бұл саясат АҚБЖ әзірлеу және ілестіру іске асырылатын ұйымның стратегиялық тәуекелдерін басқару мәтінін ескереді ме?				
4.2.1.b.5 Бұл саясат тәуекелдер деңгейі анықталатын критерийларды белгілейді ме? (4.2.1.c қараңыз))?				
4.2.1.b.6 Бұл саясатты басшылық бекітті ме?				
c) Ұйымның тәуекелдерді бағалауға қатысты ұстанымын анықтауға тиісті				
4.2.1.c.1 Пайдаланылатын АҚБЖ, бизнес-ақпарат қауіпсіздігіне қойылатын сәйкестендірілген талаптарға, сонымен қатар құқықтық және нормативтік талаптарға сәйкес келетін тәуекелдерді бағалау әдісі сәйкестендірілді ме?				
4.2.1.c.2 Тәуекелдерді қабылдау және қолданылатын тәуекел деңгейлерін анықтау үшін критерийлер әзірленді ме? (5.1.f қараңыз)				
4.2.1.c.3 Тәуекелдерді бағалаудың таңдап алынған әдісі тәуекелдерді бағалау процедураларының салыстырылатын және жаңғыртылатын нәтижелерін кепілдендіреді ме?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
d) Тәуекелдерді сәйкестендіруге тиісті				
4.2.1.d.1 Тәуекелдерді сәйкестендіру үшін процесс әзірленді ме және пайдаланылады ма?				
4.2.1.d.2 Көрсетілген процесс АҚБЖ қолдану аясына қатысты активтерді және осы активтердің иегерлерін сәйкестендіреді ме?				
4.2.1.d.3 Бұл процесс осы ресурстарға қауіпті сәйкестендіреді ме?				
4.2.1.d.4 Бұл процесс осы қауіптерді жүзеге асыру үшін пайдаланылуы мүмкін осалдықты сәйкестендіреді ме?				
4.2.1.d.5 Бұл процесс құпиялылықтың, тұтастықтың және қолжетімділіктің бұзылуынан активтерге ықпал етуі мүмкін әсерді сәйкестендіре ме?				
e) Тәуекелдерді талдау және бағалауға тиісті				
4.2.1.e.1 Тәуекелдерді талдау және бағалау үшін процесс әзірленді ме және пайдаланылады ма?				
4.2.1.e.2 Ұйым масштабында көрсетілген процесс қауіпсіздіктің бұзылуынан тигізуі мүмкін әсерді құпиялылықтың, тұтастықтың немесе ресурстарға қолжетімділіктің бұзылу салдарларын ескере отырып, бағаланады ма?				
4.2.1.e.3 Көрсетілген процесс осы ресурстармен байланысты басым болатын қатерлер, осалдықтар және әсерлер түрінде қауіпсіздіктің бұзылуын жүзеге асырудың шынайы мүмкіндігін, сонымен қатар				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
аталмыш сәтте жүзеге асырылған басқару құралдарын бағалайды ма?				
4.2.1.e.4 Көрсетілген процесс тәуекелдер деңгейін бағалайды ма?				
4.2.1.e.5 Көрсетілген процесс тәуекелдердің қолдануға жарамды болып табылатындығын немесе 4.2.1.c.2) анықталған тәуекелдерді қабылдау критериларын пайдалана отырып, өңдеуді талап ететіндігін анықтайды ма?				
f) Тәуекелдерді өңдеу нұсқаларын бағалау және сәйкестендіруге тиісті				
4.2.1.f.1 Тәуекелдерді өңдеудің нұсқаларын бағалау және сәйкестендіру үшін процесс әзірленді ме және пайдаланылады ма?				
4.2.1.f.2 Көрсетілген процесте келесі ықтимал әрекеттер қарастырылады ма: 1) басқарудың тиімді құралдарын қолдану; 2) тәуекелдерді саналы түрде және әдейі қабылдау, олардың тәуекелдерді қабылдау критериларын және ұйым саясатын анық қанағаттандыруы шартында (4.2.1.c.2 қараңыз); 3) тәуекелдердің алдын алу немесе 4) ассоциацияланған бизнес-тәуекелдерді басқа тараптарға, мысалы, сақтандырушыларға және жеткізушілерге табыстау?				
g) Тәуекелдерді өңдеу үшін басқару құралдарын және басқару мақсаттарын таңдауға тиісті				
4.2.1.g.1 Тәуекелдерді бағалау кезінде және тәуекелдерді өңдеу процесінде сәйкестендірілген талаптарды қанағаттандыратын				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
басқару құралдарын және басқару мақсаттарын таңдау және енгізу үшін процесс әзірленді ме және пайдаланылады ма?				
4.2.1.g.2 Көрсетілген таңдау процесі тәуекелдерді қабылдау критериларын (4.2.1.c), сонымен қатар құқықтық және нормативтік талаптарды, шарттық міндеттемелерді ескереді ме?				
4.2.1.g.3 Көрсетілген таңдау процесі басқару мақсаттары және басқару құралдары *ИСО/МЭК 27001:2005* стандартының А Қосымшасынан таңдап алынатындығын және олардың барлық идентификациялық талаптарды орындауға рұқсат беретіндігін кепілдендіреді ме?				
4.2.1.g.4 Көрсетілген таңдау процесі басқару мақсаттары және басқару құралдары *ИСО/МЭК 27001:2005* стандартының А қосымшасынан таңдалмауына жол береді ме?				
h) Ұсынылатын қалдық тәуекелдерді басшылықтың бекітуі тиіс				
4.2.1.h.1 Басшылықтың қалған тәуекелдерді бекітуі үшін процесс әзірленді ме және пайдаланылады ма?				
i) АҚБЖ жүзеге асыру және пайдалану үшін басшылықтан рұқсат алуы тиіс				
4.2.1.i.1 АҚБЖ жүзеге асыруға және пайдалануға басшылық рұқсатын алу үшін процесс әзірленді ме және пайдаланылады ма?				
j) «АҚБЖ басқару құралдары және мақсаттарын қолдану туралы ереже» дайындауға тиісті				
4.2.1.j.1 «..қолдану туралы ереже» дайындау үшін процесс әзірленді				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
ме және пайдаланылады ма?				
4.2.1.j.2 4.2.1.g-да таңдап алынған басқару мақсаттарын және басқару құралдарын, сонымен қатар оларды таңдау себептерін қамтитын «...қолдану туралы ереже» дайындалды ма?				
4.2.1.j.3 Көрсетілген «...қолдану туралы ереже» ағымдық сәтте жүзеге асырылған басқару құралдарын және басқару мақсаттарын қамтиды ма?				
4.2.1.j.4 Көрсетілген «...қолдану туралы ережеде» ИСО/МЭК 27001:2005 стандартының А қосымшасында аталған басқару құралдарының кез келгенінің және басқару мақсаттарының кез келгенің ерекше жағдайлары, сонымен қатар осы мақсаттар мен құралдардың ерекше жағдайларының негіздемесі тіркелді ме?				
4.2.2 АҚБЖ жүзеге асыру және пайдалану ***Ұйым:***				
а) Ақпараттық қауіпсіздік тәуекелдерін басқару үшін басшылықтың сәйкес әрекеттері, активтері, міндеттемелері және басымдылықтары идентификацияланатын тәуекелдерді өңдеу жоспарының ережелерін тұжырымдауға тиісті (5 қараңыз).				
4.2.2.a.1 Ақпараттық қауіпсіздік тәуекелдерін басқару үшін басшылықтың сәйкес әрекеттері, міндеттемелері және басымдылықтары идентификацияланатын тәуекелдерді өңдеу жоспарын тұжырымдау процесі әзірленді ме және пайдаланылады ма?				
4.2.2.a.2 Көрсетілген процесс тәуекелдерді өңдеу жоспарында				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
басшылықтың қажетті іс-әрекетін сәйкестендіруді қамтамасыз етеді ме?				
4.2.2.a.3 Көрсетілген процесс ақпараттық қауіпсіздік тәуекелдерін басқару үшін қажетті міндеттемелерді және басымдылықтарды сәйкестендіруді қамтамасыз етеді ме? (5 қараңыз)?				
b) Сәйкестендірілген басқару мақсаттарына қол жеткізу үшін тәуекелдерді өңдеу жоспарын жүзеге асыруға тиісті, бұл қаржыландыру, рольдерді бөлу және жауапкершілік мәселелерін қарастыруды қамтиды.				
4.2.2.b.1 Тәуекелдерді өңдеу жоспарын жүзеге асыру үшін процесс әзірленді ме және пайдаланылады ма?				
4.2.2.b.2 Көрсетілген процесс тәуекелдерді өңдеудің жүзеге асырылған жоспары сәйкестендірілген басқару мақсаттарына қол жеткізуді қамтамасыз етуді кепілдендіруге рұқсат береді ме?				
4.2.2.b.3 Көрсетілген процесс қаржыландыру, рольдерді бөлу және жауапкершілік мәселелерін қарастыруды қамтиды ма?				
c) Басқару мақсаттарын орындау үшін 4.2.1.g –да таңдап алынған басқару құралдарын жүзеге асыруға тиісті.				
4.2.2.c.1 4.2.1.g-да таңдап алынған басқару құралдарын енгізу процесі әзірленді ме және пайдаланылады ма?				
4.2.2.c.2 Аталған процесс басқарудың енгізілетін құралдарының басқару мақсаттарына сәйкестігін қамтамасыз етеді ме?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
d) Таңдап алынған басқару құралдарының және басқару құралдарының топтарының тиімділігін қалай өлшеу керектігін анықтау және алынған нәтижелер салыстырылатын және жаңғыртылатын болуы үшін бұл өлшеулердің басқару құралдарының тиімділігін бағалау үшін қалай пайдалануы тиістігін анықтау (4.2.3.c қараңыз))				
4.2.2.d.1 Таңдап алынған басқару құралдарының немесе басқару құралдары топтарының тиімділігін қалай өлшеу керектігін анықтауға рұқсат беретін процесс әзірленді ме және пайдаланылды ма?				
4.2.2.d.2 Аталмыш процесс осы өлшеулердің басқару құралдарының және басқару құралдары топтарының тиімділігін бағалау үшін қалай пайдаланылуы тиістігін көрсетулерді қамтиды ма?				
4.2.2.d.3 Көрсетілген процесс өлшеудің салыстырмалы және жаңғыртылатын нәтижелерін алуды қамтамасыз етеді ме? (4.2.3.c қараңыз)?				
e) Оқыту және хабарлау бағдарламаларын жүзеге асыру (5.2.2 қараңыз)				
4.2.2.e Оқыту және хабарлаудың қажетті бағдарламаларын жүзеге асыру үшін процесс әзірленді ме және пайдаланылады ма? (5.2.2 т. сәйкес)?				
f) АҚБЖ пайдалануын басқаруы тиіс				
4.2.2.f АҚБЖ пайдалануды басқару үшін процесс әзірленді ме және пайдаланылады ма?				
g) АҚБЖ арналған ресурстарды басқаруы тиіс (5.2 қараңыз)				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
4.2.2.g АҚБЖ үшін қажетті ресурстарды басқару процесі әзірленді ме және пайдаланылады ма? (5.2 т. сәйкес)?				
h)Қауіпсіздік оқиғаларын дереу айқындауды және қауіпсіздіктің оқыс оқиғаларына әрекет етуді қамтамасыз етуге рұқсат ететін процедураларды және басқа басқару құралдарын жүзеге асыруы тиіс (4.2.3а қараңыз)				
4.2.2.h Қауіпсіздік оқиғаларын дереу айқындауды және қауіпсіздіктің оқыс оқиғаларына әрекет етуді қамтамасыз етуге рұқсат ететін процедураларды және басқа басқару құралдарын жүзеге асыру үшін процесс әзірленді ме? (4.2.3 т. қараңыз)?				
4.2.3 АҚБЖ мониторингісі және талдау ***Ұйым:***				
а) Басқа басқару құралдарының және процедураларының мониторингісін және талдау процедураларын орындауға тиісті				
4.2.3.а.1 Қателіктерді, қауіпсіздікті бұзу және қауіпсіздіктің оқыс оқиғаларын талдау және мониторингісін орындауға рұқсат беретін процедураларды және басқа басқару құралдарын талдау және мониторингісі процесі әзірленді ме және пайдаланылады ма?				
4.2.3.а.2 Көрсетілген процесс өңдеу нәтижелеріндегі қателіктерді дер кезінде айқындауды қамтамасыз етеді ме?				
4.2.3.а.3 Көрсетілген процесс сәті түспеген және сәтті қауіпсіздік бұзылуларын және қауіпсіздік оқыс оқиғаларын дер кезінде сәйкестендіруді қамтамасыз етеді ме?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
4.2.3.a.4 Көрсетілген процесс басшылыққа адамдарға тапсырылған немесе ақпараттық технологиялар құралдарымен жүзеге асырылған қауіпсіздікті қамтамасыз ету бойынша әрекеттердің тиісті түрде орындалуын анықтауға мүмкіндік береді ме?				
4.2.3.a.5 Көрсетілген процесс қауіпсіздік оқиғаларын айқындауға және осындай түрде индикаторларды пайдалану жолымен қауіпсіздік оқыс оқиғаларының алдын алуға көмектеседі ме?				
4.2.3.a.6 Көрсетілген процесс қауіпсіздіктің бұзылуын жою үшін қабылданған шаралардың тиімділігін анықтауға рұқсат береді ме?				
b) Қауіпсіздік аудиттерінің нәтижелерін, оқыс оқиғаларды, тиімділікті өлшеу нәтижелерін, барлық мүдделі тараптардан алынған ұсыныстарды және ақпаратты ескерумен АҚБЖ тиімділігін тұрақты талдауды жүзеге асыру (АҚБЖ саясатын және қауіпсіздік мақсаттары қадағалауды, сонымен қатар қауіпсіздікті басқару құралдарын талдауды қосқанда)				
4.2.3.b.1 АҚБЖ тиімділігін тұрақты талдау үшін процесс әзірленді ме және пайдаланылады ма?				
4.2.3.b.2 Аталмыш процесс қауіпсіздік саясатын және басқару мақсаттарын қадағалау талдауын, сонымен қатар қауіпсіздікті басқару құралдарын талдауды қамтиды ма?				
4.2.3.b.3 Көрсетілген процесс қауіпсіздік аудиттерінің нәтижелерін, оқыс оқиғаларды, тиімділікті өлшеу нәтижелерін, барлық мүдделі тараптардан алынған ұсыныстарды және ақпаратты ескереді ме?				
c) Қауіпсіздік талаптары қанағаттандырылғанына көз жеткізу үшін басқару құралдарының тиімділігін өлшеуге тиісті.				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
4.2.3.c.1 Басқару құралдарының тиімділігін өлшеу үшін процесс әзірленді ме?				
4.2.3.c.2 Көрсетілген процесс қауіпсіздіктің сәйкестендірілген талаптарының орындалуын тексеруді қамтамасыз етеді ме?				
d) Жоспарланған кезеңдерден кейін тәуекелдердің бағалауын талдауды іске асыру және қалған тәуекелдер деңгейін және тәуекелдердің сәйкестендірілген қолайлы деңгейлерін талдау				
4.2.3.d.1 Жоспарланған кезеңдерден кейін тәуекелдердің бағалауын талдау, сонымен қатар қалған тәуекелдер деңгейін талдау және сәйкестендірілген қолайлы тәуекел деңгейлерін талдау процесі әзірленді ме және пайдаланылады ма?				
4.2.3.d.2 Көрсетілген процесс ұйымда болып жататын өзгерістерді ескереді ме?				
4.2.3.d.3 Көрсетілген процесс технологияда болып жатқан өзгерістерді ескереді ме?				
4.2.3.d.4 Көрсетілген процесс бизнес-мақсаттарда және бизнес-процестерде болып жатқан өзгерістерді ескереді ме?				
4.2.3.d.5 Көрсетілген процесс сәйкестендірілген қауіптерді ескереді ме?				
4.2.3.d.6 Көрсетілген процесс жүзеге асырылған басқару құралдарының тиімділігін ескереді ме?				
4.2.3.d.7 Көрсетілген процесс құқықтық немесе нормативтік				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
саладағы өзгерістер, шарттық міндеттемелердің өзгерістері және қоғамдық климаттағы өзгерістер секілді сыртқы оқиғаларды ескереді ме?				
e) Жоспарланған кезеңдерден кейін АҚБЖ ішкі аудиттерін жүргізуге тиісті (Стандарттың 6-Тармағын қараңыз)				
4.2.3.e Жоспарланған кезеңдерден кейін АҚБЖ ішкі аудиттерін жүргізуді қамтамасыз ететін процесс әзірленді ме (Стандарттың 6-т. сәйкес)				
f) Қолданылу саласы балама болып қалатындығын, ал АҚБЖ процесін жетілдіру сәйкестендіргенін кепілдендіру үшін басқарушы персоналмен АҚБЖ талдауын тұрақты жүргізуге тиісті (Стандарттың 7.1 т. қараңыз).				
4.2.3.f АҚБЖ процесін жетілдіруді сәйкестендіру және қолдану аясының адекваттығын сақтауды кепілдендіруге рұқсат беретін басқарушы персоналмен АҚБЖ тұрақты талдауына арналған процесс әзірленді ме және пайдаланылады ма (Стандарттың 7.1 т. сәйкес)?				
g) Мониторинг және талдау нәтижесінде алынған мәліметтерді ескеру үшін қауіпсіздік бойынша жоспарларды жаңартуға тиісті				
4.2.3.g Мониторинг және талдау нәтижесінде алынған мәліметтерді ескеруге рұқсат беретін қауіпсіздік бойынша жоспарларды жаңарту үшін процесс әзірленді ме және пайдаланылады ма?				
h) АҚБЖ тиімділігіне немесе өндірімділігі ықпал етуі мүмкін әрекеттерді және оқиғаларды тіркеуге тиісті (Стандарттың 4.3.3 қараңыз)				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
4.2.3.h АҚБЖ тиімділігіне немесе өндірімділігі ықпал етуі мүмкін әрекеттерді және оқиғаларды тіркеу үшін процес әзірленді ме және пайдаланылады ма? (Стандарттың 4.3.3 т. сәйкес)?				
4.2.4 АҚБЖ ілестіру және жетілдіру ***Ұйым тұрақты түрде тиісті:***				
a) АҚБЖ сәйкестендіріле жетілдірілуін жүзеге асыру				
4.2.4.a АҚБЖ-да сәйкестендірілген жетілдірулерді жүзеге асыру үшін процесс әзірленді ме және пайдаланылады ма?				
b) Стандарттың 8.2 және 8.3 тт. сәйкес тиісті түзетуші және ескертпелі шараларды қабылдау				
4.2.4.b.1 8.2 және 8.3 тт. сәйкес қажетті түзетуші және ескертуші шараларды қабылдау үшін процесс әзірленді ме және пайдаланылады ма?				
4.2.4.b.2 Басқа ұйымдардың, сондай-ақ ұйымның өзіндік қауіпсіздікті қамтамасыз ету тәжірибесінен алынған білімдерді қолдану үшін процесс әзірленді ме және пайдаланылады ма?				
c) Барлық мүдделі тараптарды шаралар және жетілдірулер жөнінде хабардар ету (хабарламалардың нақтылық деңгейі жағдайларға сәйкес болуы тиіс), сонымен қатар олармен болжамды әрекеттерді сәйкестендіру				
4.2.4.c.1 Барлық мүдделі тараптарды шаралар және жетілдірулер жөнінде хабардар ету үшін процесс әзірленді ме және пайдаланылады ма?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
4.2.4.c.2 Көрсетілген процесс ақпараттандырудың тиісті нақтылық деңгейін қамтамасыз етеді ме?				
4.2.4.c.3 Көрсетілген процесс болжамды әрекеттерді сәйкестендіруге арналған процедураларды қамтиды ма?				
d) Жетілдірудің қойылған мақсаттарға қол жеткізетіндігіне көз жеткізу				
4.2.4.d Жетілдірудің қойылған мақсаттарға қол жеткізетіндігіне көз жеткізуге рұқсат беретін процесс әзірленді ме және пайдаланылады ма?				
4.3 Құжаттамаға қойылатын талаптар				
4.3.1 Жалпы талаптар				
4.3.1.a Құжаттама басқару шешімдерін қамтиды ма, ол басқару шешімдері және саясаттармен әрекеттер байланысының бақылауын кепілдендіреді ме және жазылған нәтижелердің жаңғыртылуын қамтамасыз етеді ме?				
4.3.1.b Таңдап алынған басқару құралдарынан артқа тәуекелдерді бағалау және тәуекелдерді өңдеу процесінің нәтижелеріне және әрі қарай АҚБЖ саясатына және мақсаттарына дейінгі өзара байланысты көрсету мүмкіндігі бар ма?				
4.3.1.c АҚБЖ құжаттамасы қауіпсіздік саясатының құжатталған ережелерін (4.2.1.b қараңыз) және басқару мақсаттарын қамтиды ма?				
4.3.1.d АҚБЖ қолдану аясын сипаттайтын құжат бар ма (4.2.1.a				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
қараңыз)?				
4.3.1.e АҚБЖ бойынша құжаттама АҚБЖ қолдау үшін пайдаланылатын басқару құралдарын және процедураларды қамтиды ма?				
4.3.1.f АҚБЖ бойынша құжаттама тәуекелдерді бағалау әдістемесінің сипаттамасын қамтиды ма (4.2.1.c қараңыз)?				
4.3.1.g АҚБЖ бойынша құжаттамаға тәуекелдерді бағалау жөнінде есеп енеді ме (4.2.1.c – 4.2.1.g тт қараңыз)?				
4.3.1.h АҚБЖ бойынша құжаттамаға тәуекелдерді өңдеу жоспары енгізілген бе (4.2.2.b қараңыз)?				
4.3.1.i Ақпараттық қауіпсіздік процестерін тиімді жоспарлауды, пайдалануды және басқаруды қамтамасыз ету үшін және басқару құралдарының тиімділігін өлшеу тәсілін сипаттау үшін ұйымға қажетті құжатталған процедуралар қол жетімді ме? (4.2.3.c қараңыз)?				
4.3.1.j ИСО/МЭК 27001:2005 стандартымен талап етілетін жазбалар қолжетімді ме (сонымен қатар 4.3.3 қараңыз)?				
4.3.1.k АҚБЖ бойынша құжаттамаға қолданылуы туралы Ереже енгізілді ме?				
4.3.2 Құжаттарды басқару				
4.3.2.a АҚБЖ үшін қажетті құжаттарды қорғау және басқаруға арналған процесс әзірленді ме және пайдаланылады ма?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
4.3.2.b Көрсетілген процесті қолдау және құжаттарды басқару үшін басқару әсерлерін анықтау процедурасы әзірленді ме?				
4.3.2.c Көрсетілген процедура құжаттарды жариялау алдында адекваттығының критериясы бойынша құжаттарды бекіту үшін қажетті әрекеттерді анықтайды ма?				
4.3.2.d Көрсетілген процедура қажеттілігі бойынша құжаттарды талдау және жаңғыртуды және құжаттарды қайта бекітуді қамтиды ма?				
4.3.2.e Көрсетілген процедура құжаттардың ағымдық редакциясының мәртебесін және өзгертулерді сәйкестендіруді қамтамасыз етеді ме?				
4.3.2.f Көрсетілген процедура пайдалану орындарында сәйкес құжаттардың маңызды нұсқаларының қолжетімділігін қамтамасыз етеді ме?				
4.3.2.g Көрсетілген процедура құжаттардың қолайлы оқылуын және жылдам сәйкестендірілуін сақтауды қамтамасыз етеді ме?				
4.3.2.h Көрсетілген процедура құжаттарға оны қажет етушілердің қол жеткізуін, сонымен қатар құжаттардың құжаттар классификациясына сәйкес қолданылатын процедураларға сәйкес табысталуын, сақталуын және ең соңында жойылуын қамтамасыз етеді ме?				
4.3.2.i Көрсетілген процедура сырттан келген құжаттардың сәйкестендірілуін қамтамасыз етеді ме?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
4.3.2.j Көрсетілген процедура құжаттардың таратылуын бақылауды қамтамасыз етеді ме?				
4.3.2.k Көрсетілген процедура ескірген құжаттарды кездейсоқ пайдаланудың алдын алады ма?				
4.3.2.l Көрсетілген процедура егер қандай да бір мақсат үшін сақталынатын болса, құжаттардың қолайлы сәйкестендірілуін қамтамасыз етеді ме?				
4.3.3 Жазбаларды басқару				
4.3.3.a Талаптарға сәйкестік және АҚБЖ тиімді пайдалану куәлігін қамтамасыз ететін жазбаларды құруға және қолдауға арналған процесс әзірленді ме және пайдаланылады ма?				
4.3.3. b Көрсетілген процесс жазбалардың қорғалуын және басқаруды қамтамасыз етеді ме?				
4.3.3.c Көрсетілген процесс АҚБЖ-да барлық маңызды құқықтық және нормативтік талаптар, сонымен қатар шарттық міндеттемелер ескерілетіндігін кепілдендіреді ме?				
4.3.3.d Көрсетілген процесс жазбалардың қолайлы оқылуын, сәйкестендірілуін жеңілдігін және алынуын қамтамасыз етеді ме?				
4.3.3.e Жазбаларды сәйкестендіру, сақтау, қорғау, алу және жою үшін қажетті басқару құралдары құжатталды ма және жүзеге асырылды ма?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
4.3.3.f 4.2 т. анықталған процестер өнімділігінің жазбалары және АҚБЖ-мен байланысты маңызды қауіпсіздік оқыс оқиғалары барлық жағдайларының жазбалары жүргізіледі ме?				
5 Басшылықтың (басқарушы персоналдың) жауапкершілігі				
5.1 Басшылықтың бейімділігі				
5.1.a Басшылыққа АҚБЖ әзірлеу, жүзеге асыру, пайдалану, мониторингісі, талдау, ілестіру және жетілдіруге өз бейімділігін (мүдделілігін) көрсетуге рұқсат беретін процесс әзірленді ме және пайдаланылады ма?				
5.1.b Көрсетілген процесс АҚБЖ Саясатын әзірлеуге басшылықтың қатысуын қамтиды ма?				
5.1.c Көрсетілген процесс басшылықтың АҚБЖ жоспарлары мен мақсаттарын әзірлеуге қатысуын қамтамасыз етеді ме?				
5.1.d Көрсетілген процесс ақпараттық қауіпсіздік үшін рольдерді және жауапкершілікті бөлуді (басшылықпен) қамтиды ма?				
5.1.e Көрсетілген процесс ұйым қызметкерлерін ақпараттық қауіпсіздік мақсаттарына қол жеткізудің және ақпараттық қауіпсіздік саясатын қадағалаудың маңыздылығы, ұйымның заң алдындағы жауапкершілігін және ұдайы жетілдіру қажеттілігі жөнінде хабардар етуді (басшылықпен) қамтиды ма?				
5.1.f Көрсетілген процесс АҚБЖ әзірлеу, жүзеге асыру, пайдалану,				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
ілестіру және жетілдіру үшін жеткілікті ресурстарды беруді (басшылықпен) қамтиды ма (Стандарттың 5.2.1 т. сәйкес)				
5.1.g Көрсетілген процесс басшылықтың тәуекелдерді қабылдау және тәуекелдердің қолайлы деңгейлері үшін критерияларды таңдауға қатысуын қамтиды ма?				
5.1.h Көрсетілген процесс АҚБЖ ішкі аудиттерінің жүргізілуін қамтамасыз етуді қамтамасыз етеді ме (6-т. сәйкес)?				
5.1.i Көрсетілген процесс АҚБЖ басқарушылық талдауын жүргізуді қамтиды ма? (7-т. сәйкес)?				
5.2 Ресурстарды басқару				
5.2.1 талабы Ресурстарды беру				
5.2.1.a АҚБЖ үшін қажетті ресурстарды анықтау және беру үшін ұйыммен пайдаланылатын процесс әзірленді ме?				
5.2.1.b Көрсетілген процесс АҚБЖ әзірлеу, жүзеге асыру, пайдалану, мониторинг, талдау, ілестіру және жетілдіру үшін қажетті ресурстарды беруді қамтамасыз етеді ме?				
5.2.1.c Көрсетілген процесс ақпараттық қауіпсіздік процедураларымен бизнес-талаптарды қолдауды қамтамасыз ету үшін қажетті ресурстарды беруді қамтамасыз етеді ме?				
5.2.1.d Көрсетілген процесс құқықтық және нормативтік талаптарды, сонымен қатар қауіпсіздік бойынша шарттық міндеттемелерді				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
сәйкестендіру және есепке алу үшін қажетті ресурстарды беруді қамтамасыз етеді ме?				
5.2.1.e Көрсетілген процесс барлық жүзеге асырылған басқару құралдарын мүлтіксіз қолдану көмегімен адекватты қауіпсіздікті қамтамасыз ету үшін қажетті ресурстарды беруді қамтамасыз етеді ме?				
5.2.1.f Көрсетілген процесс қажеттілігі бойынша талдауды орындау үшін қажетті ресурстарды беруді және талдау нәтижелері бойынша тиісті түрде әрекет етуді қамтамасыз етеді ме?				
5.2.1.g Көрсетілген процесс АҚБЖ тиімділігін, егер қажет болса, жетілдіру үшін қажетті ресурстарды беруді қамтамасыз етеді ме?				
5.2.2 талабы Оқыту, хабардар болу және құзыреттілік				
5.2.2.a АҚБЖ-да анықталған міндеттемелер жүктелген барлық персонал қажетті міндеттерді орындау үшін тиісті квалификацияға ие екендігін кепілдендіретін процес әзірленді ме және пайдаланылады ма?				
5.2.2.b Көрсетілген процесс АҚБЖ-мен байланысты жұмыстарды орындайтын персонал квалификациясының қажетті деңгейін анықтауды қамтамасыз етеді ме?				
5.2.2.c Көрсетілген процесс оқытуды жүргізуді немесе осы қажеттіліктерді қанағаттандыру үшін басқа шараларды (мысалы, білікті маманды жалдау) қабылдауды қамтамасыз етеді ме?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
5.2.2.d Көрсетілген процесс қабылданған шаралардың тиімділігін бағалау бойынша әрекеттерді қамтиды ма?				
5.2.2.e Көрсетілген процесс білім, оқыту, дағдылар, тәжірибе және біліктілік жөнінде жазбалар жүргізуді қамтамасыз етеді ме (Стандарттың 4.3.3 т. сәйкес)?				
5.2.2.f Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметінің маңыздылығы және мәнділігі жөнінде, сонымен қатар АҚБЖ мақсаттарына қол жеткізуге қатысуы жөнінде барлық тартылған персоналдың хабардар болуын кепілдендіруге рұқсат беретін процесс әзірленді ме және пайдаланылады ма?				
6 АҚБЖ ішкі аудиттері				
6.a Жоспарланған уақыт интервалдарынан кейін АҚБЖ ішкі аудиттерін жүргізуді қамтамасыз ететін процесс әзірленді ме және пайдаланылады ма?				
6.b Аталмыш процесс АҚБЖ басқару мақсаттары, басқару құралдары, процестері және процедуралары ИСО/МЭК 27001:2005 стандартының талаптарына және сәйкес заңдарға және нормативтерге сәйкес келетіндігін анықтауға рұқсат береді ме?				
6.c Аталмыш процесс АҚБЖ басқару мақсаттары, басқару құралдары, процестері және процедуралары ақпараттық қауіпсіздіктің сәйкестендірілген талаптарына сәйкес келетіндігін анықтауға рұқсат береді ме?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
6.d Аталмыш процесс АҚБЖ басқару мақсаттары, басқару құралдары, процестері және процедуралары тиімді түрде жүзеге асырылатындығын және ілестіретіндігін анықтауға рұқсат береді ме?				
6.e Аталмыш процесс басқару мақсаттары, басқару құралдары, процестері және процедуралары күтімге сәйкес орындалуын анықтауға рұқсат береді ме?				
6.f Аудитке жататын процестердің және салалардың мәртебесін және маңыздылығын, сонымен қатар алдыңғы аудиттердің нәтижелерін ескеретін аудит бағдарламасы жоспарланды ма?				
6.g Аудит критериларын, шектерін, мерзімділігін және әдістерін қамтамасыз ететін процесс әзірленді ме және пайдаланылады ма?				
6.h Аудит процесінің объективтілігін және бейтараптылығын және аудиторларға өз жұмысының аудитын жүргізудің мүмкін еместігін кепілдендіретін аудиторларды таңдау үшін процесс әзірленді ме және пайдаланылады ма?				
6.i Аудитті жоспарлауға және жүргізуге, сонымен қатар аудит нәтижелері бойынша жазбалар жүргізуге және есептілікке қойылатын талаптарды және міндеттемелерді анықтайтын құжатталған процедура пайдаланылады ма? (Стандарттың 4.3.3 т.				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
сәйкес)?				
6.j Аудитке тиесілі аумақ үшін жауапты басқару персоналының тарапынан айқындалған сәйкессіздіктерді және олардың себептерін жою бойынша кезек күттірмейтін шаралар қабылдануын қамтамасыз ететін процесс әзірленді ме және пайдаланылады ма?				
6.k Кейінгі шаралар (follow-up activities) Стандарттың 8-т. сәйкес тексеру нәтижелері бойынша есепті құру және қабылданған шараларды тексеруді қамтитындығын кепілдендіретін процесс әзірленді ме және пайдаланылады ма?				
7 Басшылықтың АҚБЖ қайта қарауы (талдау)				
7.1 Жалпы ережелер				
7.1.a Тұрақты қолданылуын, адекваттығын және тиімділігін қамтамасыз ету мақсатында жоспарланған уақыт интервалдарынан кейін (жылына бір реттен кем емес) АҚБЖ талдауын жүргізуді кепілдендіретін процесс әзірленді ме және пайдаланылады ма?				
7.1.b Көрсетілген талдау АҚБЖ жетілдіру мүмкіндіктерін және өзгертулердің қажеттілігін, соның ішінде ақпараттық қауіпсіздік саясатын және ақпараттық қауіпсіздік мақсаттарын анықтауды қамтиды ма?				
7.1.c Талдау нәтижелері анық түрде құжатталады ма және сәйкес жазбалар жүргізіледі ме (4.3.3 т. сәйкес)?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
7.2 Талдауға арналған бастапқы деректер				
7.2.a Басшылықпен талдау үшін бастапқы деректерге барлық қажетті ақпаратты қосуға рұқсат беретін процесс әзірленді ме және пайдаланылады ма (басқарма талдауы)?				
7.2.b Көрсетілген процесс АҚБЖ талдауын және аудиттер нәтижелерін басқарма талдауы үшін бастапқы деректер ретінде пайдалануды қамтамасыз етеді ме?				
7.2.c Көрсетілген процесс мүдделі тараптардың ұсыныстарын және ескертулерін басқарма талдауы үшін бастапқы деректер ретінде пайдалануды қамтамасыз етеді ме?				
7.2.d Көрсетілген процесс басқарма талдауына арналған бастапқы деректер ретінде АҚБЖ өнімділігін және тиімділігін арттыру үшін ұйымда пайдаланылуы мүмкін әдістер, өнімдер немесе процедуралар жөнінде ақпаратты пайдалануды қамтамасыз етеді ме?				
7.2.e Көрсетілген процесс алдын алу және түзету шараларының мәртебесі жөніндегі ақпаратты басқарма талдауы үшін бастапқы деректерге енгізуді қамтамасыз етеді ме?				
7.2.f Көрсетілген процесс тәуекелдерді алдыңғы бағалау кезінде адекватты түрде ескерілмеген осалдықтар немесе қауіптер туралы ақпаратты басқарма талдауы үшін бастапқы деректер ретінде пайдалануды қамтамасыз етеді ме?				
7.2.g Көрсетілген процесс тиімділікті өлшеу нәтижелерін басқарма				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
талдауы үшін бастапқы деректер ретінде пайдалануды қамтамасыз етеді ме?				
7.2.h Көрсетілген процесс алдыңғы басқарма талдауының нәтижелері бойынша қабылданған шаралар туралы ақпаратты басқарма талдауы үшін бастапқы деректер ретінде пайдалануды қамтамасыз етеді ме?				
7.2.i Көрсетілген процесс АҚБЖ-ға ықпал ете алатын барлық өзгертулер туралы ақпаратты басқарма талдауы үшін бастапқы деректер ретінде пайдалануды қамтамасыз етеді ме?				
7.2.j Көрсетілген процесс жетілдіру бойынша нұсқауларды басқарма талдауы үшін бастапқы деректер ретінде пайдалануды қамтамасыз етеді ме?				
7.3 Талдау қорытындылары				
7.3.a Басқарма талдауының қорытындыларына АҚБЖ басқарма талдауымен байланысты барлық қажетті шешімдерді және шараларды енгізуге рұқсат беретін процесс әзірленді ме және пайдаланылады ма?				
7.3.b Көрсетілген процесс АҚБЖ тиімділігін арттырумен барлық қажетті шешімдерді және шараларды басқарма талдауының қорытындыларына енгізуді қамтамасыз етеді ме?				
7.3.c Көрсетілген процесс тәуекелдерді және тәуекелдерді өңдеу жоспарын бағалауды жаңғыртумен байланысты барлық қажетті				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
шешімдерді және шараларды басқарма талдауының қорытындыларына енгізуді қамтамасыз етеді ме?				
7.3.d Көрсетілген процесс ақпараттық қауіпсіздікке әсер етуші басқару құралдарын және процедураларды түрлендірумен байланысты барлық қажетті шешімдерді және шараларды басқарма талдауының қорытындыларына енгізуді қамтамасыз етеді ме?				
7.3.e Көрсетілген түрлендіру ақпараттық қауіпсіздікке әсер етуші басқару құралдарын және процедураларды, АҚБЖ-ға әсер етуі мүмкін ішкі және сыртқы оқиғаларға әрекет етуді, соның ішінде төменде берілгендердегі өзгертулерді қамтиды ма: i) бизнес-талаптар; ii) қауіпсіздік талаптары; iii) бар бизнес-талаптарға ықпал етуші бизнес-процесстер; iv) нормативтік немесе құқықтық талаптар; v) шарттық міндеттемелер және vi) тәуекел деңгейлері және/немесе тәуекелдерді қабылдау критериялары?				
7.3.f Көрсетілген процесс ресурстардағы қажеттіліктерді анықтаумен байланысты барлық қажетті шешімдерді және шараларды басқарма талдауының қорытындыларына енгізуді қамтамасыз етеді ме?				
7.3.g Көрсетілген процесс басқару құралдарының тиімділігін өлшеудің бар тәсілдерін жетілдірумен байланысты барлық қажетті				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
шешімдерді және шараларды басқарма талдауының қорытындысына енгізуді қамтамасыз етеді ме?				
8 АҚБЖ жетілдіру				
8.1 Ұдайы жетілдіру				
8.1.a Ақпараттық қауіпсіздік саясатын, ақпараттық қауіпсіздік мақсаттарын, аудит нәтижелерін, бақыланатын оқиғаларды талдауды, түзетуші және алдын алушы ықпалдарды, сонымен қатар басқарма талдауын пайдалану арқылы ұйыммен АҚБЖ тиімділігін ұдайы арттыруды қамтамасыз ететін процесс әзірленді ме және пайдаланылады ма (Стандарттың 7-т. сәйкес)?				
8.2 Түзетуші ықпал				
8.2.a Сәйкессіздіктің қайта пайда болуын болдырмас үшін АҚБЖ талаптарына сәйкессіздік себептерін жоюға арналған шараларды қабылдауды қамтамасыз ететін процесс әзірленді ме және пайдаланылады ма?				
8.2.b Түзетуші ықпалдар үшін құжатталған процедура әзірленді ме және пайдаланылады ма?				
8.2.c Көрсетілген процедура сәйкессіздік сәйкестендірілуін қамтамасыз етеді ме?				
8.2.d Көрсетілген процедура сәйкессіздік себептерін анықтауды қамтамасыз етеді ме?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
8.2.e Көрсетілген процедура сәйкессіздіктің қайта пайда болу мүмкіндігін болдырмайтын ықпалдардың қажеттілігін бағалауды қамтамасыз етеді ме?				
8.2.f Көрсетілген процедура қажетті түзетуші ықпалдарды анықтауды және жүзеге асыруды қамтамасыз етеді ме?				
8.2.g Көрсетілген процедура қабылданған ықпалдар нәтижелерін тіркеуді қамтамасыз етеді ме? (4.3.3 т. сәйкес)?				
8.2.h Көрсетілген процедура қабылданған түзетуші ықпалдардың талдауын қамтамасыз етеді ме?				
8.3 Ескертуші ықпал				
8.3.a Сәйкессіздіктердің пайда болуын болдырмас үшін АҚБЖ талаптарына мүмкін болатын сәйкессіздіктер себептерін болдырмауға арналған шараларды анықтауға рұқсат беретін процесс әзірленді ме және пайдаланылады ма?				
8.3.b Көрсетілген процесс әлеуетті проблемалардың ықпал жасау деңгейінің қабылданатын ескертуші шараларының адекваттығын қамтамасыз етеді ме?				
8.3.c Ескертуші ықпалдарға арналған құжатталған процедура әзірленді ме және пайдаланылады ма?				
8.3.d Көрсетілген процедура әлеуетті сәйкессіздіктердің сәйкестендірілуін және оның себептерін қамтамасыз етеді ме?				

Стандарттың тексерілетін талабы	Стандарт талабын орындауды бағалау			Стандарт талаптарын орындау бойынша нұсқаулар
	ИӘ (толық орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
8.3.e Көрсетілген процедура сәйкессіздіктердің пайда болуының алдын алу үшін ықпал жасау қажеттілігін бағалауды қамтамасыз етеді ме?				
8.3.f Көрсетілген процедура қажетті ескертуші ықпалдарды анықтауды және жүзеге асыруды қамтамасыз етеді ме?				
8.3.g Көрсетілген процедура қабылданған ықпал жасау нәтижелерін тіркеуді қамтамасыз етеді ме? (4.3.3 т. сәйкес)?				
8.3.h Көрсетілген процедура қабылданған ескертуші ықпалды талдауды қамтамасыз етеді ме?				
8.3.i Елеулі түрде өзгерген тәуекелдерге ерекше көңіл бөле отырып, ескертуші ықпалдарға қойылатын талаптарды және өзгерген тәуекелдерді сәйкестендіруге ұйымға рұқсат беретін процесс әзірленді ме және пайдаланылады ма?				
8.3.j Тәуекелдерді бағалау нәтижелерінің негіздемесіне ескертуші ықпалдардың басымдылығын анықтауды қамтамасыз ететін процесс әзірленді ме және пайдаланылады ма?				

2-кесте – ИСО/МЭК 27001:2005 стандартының А қосымшасы

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындал майды)**	
А.5 Қауіпсіздік саясаты				
А.5.1 Ақпараттық қауіпсіздік саясаты ***Ұйым:***				
Ақпараттық қауіпсіздік үшін бизнес-талаптарға және сәйкес заңдарға және нормативтерге сәйкес басқарушы персонал тарапынан қолдауды және басқаруды қамтамасыз етуге тиісті.				
А. 5.1.1. Ақпараттық қауіпсіздік саясаты туралы құжат ұйым басшылығымен бекітіліп, жарияланды ма және барлық қызметкерлердің және релеванттық сыртқы тараптардың назарына ұсынылды ма?				
А.5.1.2 Жоспарланған уақыт кезеңдерінен кейін немесе елеулі өзгерістердің пайда болуы жағдайында тұрақты қолданылуын, адекваттығын және тиімділігін қамтамасыз ету үшін ақпараттық қауіпсіздік саясатын талдау жүргізіледі ме?				
А.6 Ақпараттық қауіпсіздіктің ұйымдық аспектілері				
А.6.1 Ішкі ұйымдық аспектілер ***Ұйым:***				
ұйымдағы ақпараттық қауіпсіздікті басқаруға тиісті.				
А.6.1.1 Басшылық ақпараттық қауіпсіздік үшін мүдделілікті, тікелей тағайындауды және жауапкершілікті тануды тікелей көрсету,				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
демонстрациялау жолымен ұйымдағы қауіпсіздікке белсенді қолдауды қамтамасыз етеді ме?				
А.6.1.2 Ақпараттық қауіпсіздік бойынша қызмет сәйкес келетін рольдермен және жұмыс функцияларымен бірге ұйымның әртүрлі бөлім өкілдерімен үйлестірілген бе?				
А.6.1.3 Ақпараттық қауіпсіздікті қамтамасыз ету бойынша міндеттерді дәл анықтау жүргізілді ме?				
А.6.1.4 Ақпаратты өңдеудің жаңа құралдарын басшылықтың бекіту процесі анықталып, жүзеге асырылды ма?				
А.6.1.5 Ақпаратты қорғауға деген ұйым қажеттіліктерін көрсететін құпиялылық немесе дабыраламау жөніндегі келісімдерге қойылатын талаптар сәйкестендірілді ме және осы талаптарды ұдайы қайта қарау жүзеге асырылды ма?				
А.6.1.6 Сәйкес өкілетті ұйымдармен тиісті қатынастар ұсталынады ма?				
А.6.1.7 Ақпараттық қауіпсіздік бойынша мамандардың мамандандырылған топтарымен немесе басқа форумдарымен және кәсіби бірлестіктермен тиісті қатынастар ұсталынады ма?				
А.6.1.8 Жоспарланған уақыт интервалдары сайын немесе қауіпсіздікті жүзеге асырудағы елеулі өзгерістер жағдайында ұйымның ақпараттық қауіпсіздікті басқаруға әдістемесін тәуелсіз талдау, сонымен қатар осы әдістемені жүзеге асыруды талдау (яғни				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
ақпараттық қауіпсіздікті басқару мақсаттары, басқару құралдары, саясаттары, процестері және процедуралары) жүргізіледі ме?				
А.6.2 Сыртқы ұйымдық аспектілер ***Ұйым:***				
Қол жетімді, өңделетін, танымал немесе басқа ұйымдармен басқарылатын ұйым ақпаратын өңдеу құралдарының және ақпараттың қауіпсіздігін қамтамасыз етуге тиісті.				
А.6.2.1 Сыртқы ұйымдар тартылған бизнес-процестерде туындаған ұйым ақпаратын өңдеу құралдары мен ақпарат үшін тәуекелдер сәйкестендірілді ме және осы ақпаратқа және құралдарға жол ашылғанға дейін тиісті басқару құралдары жүзеге асырылды ма?				
А.6.2.2 Ақпаратқа немесе ұйым ресурстарына қатынауды тапсырыс берушіге берудің алдында барлық идентификациялық қауіпсіздік талаптары ескерілді ме?				
А.6.2.3 Ұйым ақпараты немесе ақпаратты өңдеу құралдары қолжетімділігін, өңделуін, пайдаланылуын, басқарылуын не ақпаратты өңдеу құралдарына өнімдерді немесе сервистерді қосуды қарастыратын басқа ұйымдармен келісімдерде барлық қажетті қауіпсіздік талаптары ескеріледі ме?				
А.7 Ресурстарды басқару				
А.7.1 Ресурстарға жауапкершілік ***Ұйым:***				
Ұйым ресурстарының тиісті қорғанысын қамтамасыз етуге және қолдауға тиісті.				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
А.7.1.1 Барлық ресурстар анық сәйкестендірілді ме? Барлық маңызды ресурстардың тізімдемесі құрылды ма және өзекті күйде ұсталынады ма?				
А.7.1.2 Ақпаратты өңдеу құралдарымен байланысты барлық ақпарат және ресурстар ұйымның өкілетті бөлімшесінің «иелігінде» [1] ме?				
А.7.1.3 Ақпаратты өңдеу құралдарымен байланысты ақпаратты және ресурстарды жол берілетін пайдалану ережелері идентификацияланып, құжатталды ма және жүзеге асырылды ма?				
А.7.2 Ақпараттар классификациясы ***Ұйым:***				
Ақпаратты қорғаудың тиісті деңгейі қамтамасыз етілгендігін кепілдендіруге тиісті.				
А.7.2.1 Ақпарат маңыздылық, құқықтық талаптар, ықпалдарды сезгіштік және сыншылдық секілді көрсеткіштер бойынша ұйым үшін классификацияланды ма?				
А.7.2.2 Ұйымда қабылданған классификация жүйесіне сәйкес ақпаратпен жұмыс істеу және таңбалау үшін процедуралардың тиісті жинағы әзірленді ме және жүзеге асырылды ма?				
А.8 Персоналмен байланысты қауіпсіздік аспектілері				
А.8.1 Жұмысқа қабылдағанға дейін ***Ұйым:***				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
Тараптық ұйымдардың қызметкерлері, мердігерлері және пайдаланушылары өз жауапкершілігін түсінетіндігін және оларға арналған рольдер үшін сәйкес келетіндігін, сонымен қатар жабдықтың ұрлануы, алаяқтық немесе дұрыс пайдаланбау қаупін төмендетуді кепілдендіруге тиісті.				
А.8.1.1 Тараптық ұйымдар қызметкерлерінің, мердігерлерінің және пайдаланушыларының жауапкершілігі және қауіпсіздігі рольдерін ұйымның ақпараттық қауіпсіздігі саясатына сәйкес анықталуы және құжатталуы жүргізіледі ме?				
А.8.1.2 Бос жұмыс орындарына үміткерлердің, тараптық ұйымдар мердігерлерінің және пайдаланушыларының барлығының персоналды деректері сәйкес заңдарға, нормативтік құжаттарға және этикалық нормаларға сәйкес, сонымен қатар жол ашылатын ақпарат категорияларын, бизнес-талаптарды ескере отырып және зерделенетін тәуекелдерге сәйкес тексеру орындалады ма?				
А.8.1.3 Тараптық ұйымдар қызметкерлерінің, мердігерлерінің және пайдаланушыларының келісім-шарттық міндеттемелеріне жалдау туралы келісім-шартының ережелерін және шарттарын қабылдау және қол қою міндеттемесі кіре ме? Және осы келісім-шартта ақпараттық қауіпсіздік үшін олардың жауапкершілігі және ұйымның жауапкершілігі белгіленеді ме?				
А.8.2 Жалдау кезінде ***Ұйым:***				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
Тараптық ұйымдардың қызметкерлері, мердігерлері және пайдаланушылары ақпараттық қауіпсіздік қатерлері және оның мәні туралы, өз жауапкершілігі және міндеттемелері туралы хабардар етілуі, өзінің әдеттегі жұмыс процесінде ұйым қауіпсіздігі саясатын қолдауға, сонымен қатар субъективті қателіктер тәуекелін төмендетуге қабілеттілігін кепілденділуі тиіс.				
А.8.2.1 Тараптық ұйымдардың қызметкерлері, мердігерлері және пайдаланушылары ақпараттық қауіпсіздік ережелерін ұйымда белгіленген саясаттарға және процедураларға сәйкес қолдануын басшылық талап етеді ме?				
А.8.2.2 Ұйымның барлық қызметкерлері және қажет болғанда, тараптық ұйымдардың мердігерлері және пайдаланушылары өз жұмыс қызметтерін орындау үшін қажетті көлемде ұйым саясатының және процедураларының жаңартылуы жөнінде тиісті ақпаратты және хабардар ететін оқытуды ала ма?				
А.8.2.3 Қауіпсіздікті бұзған қызметкерлер үшін формальды тәртіптік процесс анықталды ма?				
А.8.3 Жұмыстан босату немесе жалдау шарттарының өзгеруі ***Ұйым:***				
Тараптық ұйымдардың қызметкерлері, мердігерлері және пайдаланушылары белгіленген тәртіпте ұйымнан кететіндігін немесе жалдау шарттарын өзгертетіндігін кепілдендіруі тиіс.				
А.8.3.1 Қызметкерлерді жұмыстан босату немесе жалдау шарттарын өзгерту процедураларын орындау үшін жауапкершілік анықталып және белгіленді ме?				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
А.8.3.2 Жұмыстан босатылғанда немесе келісім-шарттың (келісім) жарамдылық мерзімі аяқталысымен тараптық ұйымдардың барлық қызметкерлері, мердігерлері және пайдаланушылары билігінде болған барлық ұйым ресурстарын қайтаруға міндетті ме?				
А.8.3.3 Жұмыстан босатылу, келісім-шартты немесе келісімдерді тоқтату жағдайында тараптық ұйымдардың барлық қызметкерлерінің, мердігерлерінің және пайдаланушыларының ақпаратқа және ақпаратты өңдеу құралдарына қол жеткізу құқықтарының күші жойылады ма және көрсетілген қол жеткізу құқықтары жалдау шарттары өзгерген жағдайда өзгереді ме?				
А.9 Жеке қауіпсіздік және қызмет ету ортасының қауіпсіздігі				
А.9.1 Қорғалған салалар ***Ұйым:***				
Ұйымның территориясына, жабдыққа және ақпаратқа рұқсат етілмеген күштеп енудің алдын алуға тиісті.				
А.9.1.1 Ақпарат және ақпаратты өңдеу құралдары орналасқан облыстарды қорғау үшін қауіпсіздік периметрлері (карта бойынша кіру жүйесімен жабдықталған кіру, қабырғалар секілді кедергілер немесе кірушілерді арнайы персоналмен бақылау) пайдаланылады ма?				
А.9.1.2 Қорғалатын облыстар сәйкес өкілеттік алған персоналмен ғана енуді қамтамасыз етуге рұқсат беретін, орындарға енуді бақылаудың қажетті құралдарымен қорғалған ба?				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
А.9.1.3 Офистерді, бөлмелерді және жабдықтарды қорғау үшін жеке қауіпсіздік шаралары әзірленіп, енгізілді ме?				
А.9.1.4 Өрттен, су басудан, жер сілкінісінен, жарылыстан, азаматтық тәртіпсіздіктерден және табиғи және антропогенді катастрофалардың басқа формаларынан жеке қорғау шаралары әзірленіп, енгізілді ме?				
А.9.1.5 Жеке қорғау шаралары және қорғалған облыстардағы жұмыс бойынша нұсқаулар әзірленіп, енгізілді ме?				
А.9.1.6 Тиеу және түсіруге арналған алаңқайлар секілді еркін ену орындары және өкілеттенбеген тұлғалардың енуі мүмкін басқа орындарды бақылау жүзеге асырылады ма? Және көрсетілген орындар мүмкіндігінше рұқсат етілмеген енудің алдын алу мақсаттарында ақпаратты өңдеу құралдарынан оқшауландырады ма?				
А.9.2 Жабдықты қорғау ***Ұйым:***				
Ресурстардың жоғалуын, зақымдалуын, ұрлануын немесе атына кір келтірушілік, ұйым қызметіндегі іркілісті болдырмауы тиіс.				
А.9.2.1 Сыртқы ортаның әсерімен байланысты тәуекелдерді және нұқсандарды, сонымен қатар рұқсат етілмеген ену мүмкіндігін төмендету үшін жабдықты орналастыру немесе қорғау жүзеге асырылады ма?				
А.9.2.2 Жабдық электр қоректендіру жүйесіндегі іркілістерден және ұсталынатын инфрақұрылымдағы іркілістер себепті туындаған басқа				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
олқылықтардан қорғалған ба?				
А.9.2.3 Деректерді беру немесе ақпараттық сервистерді қолдау үшін пайдаланылатын кабельді электр қоректендіру және телекоммуникация жүйелері тыңдалудан немесе зақымдалудан қорғалған ба?				
А.9.2.4 Жабдықтың ұдайы қолжетімділігін және тұтастығын кепілдендіруге рұқсат беретін жабдықтың тиісті ілестірілуі қамтамасыз етіледі ме?				
А.9.2.5 Ұйым сыртында жабдыққа ұйымның аумағынан тыс жұмыстың әртүрлі тәуекелдерін ескеретін қауіпсіздік шаралары қолданылады ма?				
А.9.2.6 Ақпарат тасымалдаушыларынан тұратын жабдықтардың барлық бірліктері жоюдың алдында барлық деректердің және лицензиялық бағдарламалық қамтамасыз етудің олардан жойылғандығын немесе басқа ақпаратпен сенімді ауыстырылғандығын кепілдендіру үшін тексеріледі ме?				
А.9.2.7 Жабдықты, ақпаратты немесе бағдарламалық қамтамасыз етуді ұйым шегінен шығаруға басшылықтың санкциясы талап етіледі ме?				
А.10 Коммуникацияларды және жұмыс істеуді басқару				
А.10.1 Операциялық процедуралар және жауапкершілік ***Ұйым:***				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
Ақпаратты өңдеу құралдарының түзетілген және қорғалған қызметін қамтамасыз етуге тиісті.				
А.10.1.1 Операциялық процедуралар құжатталған ба? Олардың ілестірілуі, сонымен қатар оларды қажет ететін барлық пайдаланушылар үшін қолжетімділігі қамтамасыз етілген бе?				
А.10.1.2 Ақпаратты өңдеу жүйелеріндегі және құралдарындағы өзгертулер бақылауға алынады ма?				
А.10.1.3 Ұйым ресурстарын рұқсат етілмеген немесе аңдаусыз түрлендіру немесе тиісті емес пайдалану мүмкіндігін төмендету үшін міндеттер және жауапкершілік аймақтары бөлінген бе?				
А.10.1.4 Рұқсат етілмеген ену тәуекелдерін немесе операция жүйесінің өзгерістерін төмендету үшін әзірлеу, тестілеу құралдары және өндірістік құралдар бөлінген бе?				
А.10.2 Тараптық ұйымдар сервистерінің берілуін басқару ***Ұйым:***				
Тараптық ұйыммен сервистерді жеткізу туралы келісімдерге сәйкес сервистерді беру және ақпараттық қауіпсіздіктің тиісті деңгейін жүзеге асыруға және қолдауға тиісті.				
А.10.2.1 Тараптық ұйыммен сервистерді жеткізу туралы келісімге енгізілген қауіпсіздікті басқару құралдары, сервистерді және жеткізу деңгейлерін анықтау құралдары тараптық ұйыммен жүзеге асырылғандығын, қызмет ететіндігін және ілестірілетінін кепілдендіруге рұқсат беретін процедуралар әзірленді ме?				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
А.10.2.2 Тараптық ұйыммен берілетін сервистер, есептер және жазбалар тұрақты мониторингіге және талдауға ұшыратылады ма және аудиттер тұрақты түрде жүргізіледі ме?				
А.10.2.3 Ақпараттық қауіпсіздік саясаттарын, процедураларын және басқару құралдарын ілестіру және жетілдіруді қоса алғанда сервистерді берудегі өзгерістерді басқару іске асырылады ма және бұл жағдайда тартылған бизнес-жүйелердің және процестердің сыншылдығы, сонымен қатар тәуекелдерді қайта бағалау ескеріледі ме?				
А.10.3 Жүйелерді жоспарлау және оларды қабылдау ***Ұйым:***				
Жүйелердің жұмыс істемеу тәуекелін азайтуға тиісті.				
А.10.3.1 Ресурстарды пайдалануды оңтайландыру және мониторингісі жүргізіледі ме? Жүйенің қажетті өндірімділігін қамтамасыз ету мақсатында болашақ қажеттіліктердің болжамдары құрылады ма?				
А.10.3.2 Жаңа ақпараттық жүйелерді қабылдау, модернизациялау және жаңа нұсқаларының критериялары белгіленген бе және оны әзірлеу кезінде, бірақ жүйені қабылдағанға дейін жүйенің тиісті тестілеуі орындалады ма?				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындал майды)	
А.10.4 Зиянды және мобильді бағдарламалық кодтан қорғау ***Ұйым:***				
Бағдарламалық қамтамасыз етудің және ақпараттың тұтастығын қамтамасыз етуге тиісті.				
А.10.4.1 Зиянды бағдарламалық кодтан қорғауды қамтамасыз ететін айқындау, алдын алу және қалпына келтіру құралдары, сонымен қатар пайдаланушыларды хабардар етудің тиісті процедуралары жүзеге асырылған ба?				
А.10.4.2 Мобильді кодты пайдалану рұқсат етілген жерде пайдаланылатын конфигурация санкцияланған мобильді кодтың айқын берілген қауіпсіздік саясатына сәйкес жұмыс істейтіндігін, ал рұқсат етілмеген мобильді кодтың пайдалануына жол берілмейтіндігі кепілдендіреді ме?				
А.10.5 Резервті көшірме ***Ұйым:***				
Ақпараттың және ақпаратты өңдеу құралдарының тұтастығын және қолжетімділігін қамтамасыз етуге тиісті.				
А.10.5.1 Ақпараттың және бағдарламалық қамтамасыз етудің резервті көшірмелерін тұрақты құру және тестілеу резервті көшірме саясатына сәйкес орындалады ма?				
А.10.6 Желілердің қауіпсіздігін басқару ***Ұйым:***				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
Желілердегі ақпаратты қорғауды және ұсталынатын инфрақұрылымды қорғауды қамтамасыз етуге тиісті.				
А.10.6.1 Қауіптерден қорғау мақсатында және жүйелердің және желі бойынша берілетін ақпаратты қоса қанда желіні пайдаланатын қосымшалардың қауіпсіздігін қолдау үшін желілерді тиісті басқару және бақылау жүзеге асырылады ма?				
А.10.6.2 Қауіпсіздік құралдарына, сервис деңгейлеріне қойылатын талаптарға және барлық желілік сервистер үшін басқару бойынша талаптар сәйкестендірілген ба және осы талаптар желілік сервистерге қатысты барлық келісімдерге, бұл желілердің ұйымның өз күшімен немесе сыртқы ұйымдармен (аутсорсинг) берілетіндігіне тәуелсіз, енгізілді ме?				
А.10.7 Ақпарат тасымалдаушыларын басқару және оларды қорғау ***Ұйым:***				
Ақпараттық ресурстардың зақымдалуын және ұйым жұмысының тоқтауын болдырмауға тиісті.				
А.10.7.1 Ақпаратты алынбалы тасымалдаушылармен басқару процедуралары белгіленді ме?				
А.10.7.2 Қажетсіз ақпарат тасымалдаушылары формалды процедураларды қадағалай отырып, қауіпсіз және сенімді тәсілмен жойылады ма?				
А.10.7.3 Рұқсат етілмеген ашудан немесе тиісті емес пайдаланудан ақпаратты қорғау үшін арналған ақпаратты сақтау және ақпаратпен				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындал майды)	
жұмыс істеу процедуралары белгіленген бе?				
А.10.7.4 Жүйелік құжаттаманы рұқсат етілмеген енуден қорғау жүзеге асырылады ма?				
А.10.8 Ақпарат алмасу ***Ұйым:***				
Ұйым ішінде және кез келген сыртқы нысандармен ақпарат алмасу нысанасы болып табылатын бағдарламалық қамтамасыз ету және ақпарат қауіпсіздігін қамтамасыз ету.				
А.10.8.1 Барлық типтегі коммуникация құралдарын пайдаланумен ақпарат алмасуды қорғау үшін арналған алмасу процедуралары және формалды саясаттар, сонымен қатар алмасуды басқару құралдары орнатылған ба?				
А.10.8.2 Ұйым және сыртқы ұйымдар арасында ақпарат және бағдарламалық қамтамасыз етумен алмасу туралы келісімдер жасалған ба?				
А10.8.3 Ұйым территориясының шегінде тасымалдау кезінде ақпараттан тұратын тасымалдаушылар рұқсат етілмеген енуден, тиісті емес пайдаланудан немесе зақымдалудан қорғалады ма?				
А.10.8.4 Электронды хабарламалармен жүйелерде айналатын ақпарат тиісті түрде қорғалады ма?				
А.10.8.5 Бизнестің ақпараттық жүйелерін біріктірумен байланысты ақпаратты қорғау үшін саясаттар және процедуралар әзірленіп, жүзеге асырылады ма?				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындал майды)**	
А.10.9 Электронды коммерция сервистері ***Ұйым:***				
Электронды коммерция сервистерінің қауіпсіздігін, сонымен қатар оларды қауіпсіз пайдалануды қамтамасыз етуге тиісті.				
А.10.9.1 Электронды коммерцияда пайдаланылатын және ортақ қолжетімді желілер арқылы өтетін ақпарат алаяқтық әрекеттерден, келісім-шарт бойынша даулардан, рұқсат етілмеген дабыралаудан және түрлендіруден қорғалады ма?				
А.10.9.2 Толық емес берілуді, қате бағдарлауды, хабарламалардың рұқсат етілмеген айырбасын, рұқсат етілмеген дабыралауды, хабарламалардың рұқсат етілмеген көшірмесін немесе жаңғыртылуын болдырмау мақсатында онлайн операцияларында (нақты уақытта орындалатын) пайдаланылатын ақпаратты қорғау іске асырылады ма?				
А.10.9.3 Ортақ қолжетімді жүйелерде айналатын ақпараттың тұтастығы рұқсат етілмеген түрлендіруден қорғалады ма?				
А.10.10 Мониторинг ***Ұйым:***				
Ақпаратты өңдеу бойынша рұқсат етілмеген әрекетті ашуға тиісті.				
А.10.10.1 Пайдаланушылардың әрекетін, ақпараттық қауіпсіздіктің ерекше жағдайларын және оқиғаларын тіркейтін журналдарды осы журналдарды болашақ зерттеулер және қолжетімділікті басқару мониторингісі кезінде пайдалану мақсатында жүргізу және				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындал майды)	
белгіленген кезең бойы сақтау іске асырылады ма?				
А.10.10.2 Ақпаратты өңдеу құралдарын пайдалану мониторингісінің процедуралары белгіленген бе және мониторинг нәтижелерін тұрақты талдау жүргізіледі ме?				
А.10.10.3 Журналдарды жүргізу құралдары және журналдардың ақпараты құпия ықпалдардан және рұқсат етілмеген енулерден қорғалады ма?				
А.10.10.4 Жүйелік әкімгерінің және жүйе операторының әрекеттері сәйкес журналдарда тіркеледі ме?				
А.10.10.5 Журналда іркілістерді тіркеу іске асырылады ма, олардың талдауы жүргізіледі ме және сәйкес шаралар қабылданады ма?				
А.10.10.6 Ұйым аясында немесе дәл уақыттың белгіленген көзі бойынша қауіпсіздік доменінде ақпаратты өңдеудің барлық маңызды жүйелерінің сағаты синхрондалады ма?				
А.11 Қатынауды басқару				
А.11.1 Қатынауды басқаруға қойылатын бизнес-талаптар ***Ұйым:***				
Ақпаратқа қатынауды басқаруы тиісті.				
А.11.1.1 Бизнес және қауіпсіздік тарапынан қатынауға қойылатын талаптарға негізделген қатынауды басқару саясаты белгіленіп,				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
құжатталған ба және осы саясатты тұрақты қайта қарау іске асырылады ма?				
А.11.2 Пайдаланушылардың қол жеткізуін басқару ***Ұйым:***				
Пайдаланушылардың санкцияланған қатынауын қамтамасыз ету және ақпараттық жүйелерге рұқсат етілмеген қатынаудың алдын алу.				
А.11.2.1 Барлық ақпараттық жүйелерге және сервистерге қолжетімділікті беру және күшін жою үшін пайдаланушыларды тіркеу және тіркеуден бас тартудың формальды процедурасы белгіленген бе?				
А.11.2.2 Өкілеттіктерді беру және пайдалану шектелген және бақыланатын болып табылады ма?				
А.11.2.3 Парольдерді тағайындау формальды басқару процесі арқылы бақыланады ма?				
А.11.2.4 Тұрақты уақыт интервалдары сайын басшылық формальды процесті пайдалана отырып, пайдаланушылардың қолжеткізу құқығын қайта қарастырады ма?				
А.11.3 Пайдаланушылардың жауапкершілігі ***Ұйым:***				
Пайдаланушылардың рұқсат етілмеген қатынауын, сонымен қатар ақпаратты және ақпаратты өңдеу құралдарының ұрлануын немесе беделіне нұқсан келуін болдырмауға тиісті.				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
А.11.3.1 Пайдаланушылар парольдерді таңдау және пайдалану кезінде тәжірибеде өзінің тиімділігін дәлелдеген қауіпсіздік принциптерін ұстануға міндетті ме?				
А.11.3.2 Пайдаланушылар қараусыз қалдырылған жабдықтың тиісті қорғалуын қамтамасыз етуге міндетті ме?				
А.11.3.3 Ақпараттың алынбалы тасымалдаушылары және қағаз үшін «таза стол» саясаты және ақпаратты өңдеу құралдары үшін «таза экран» саясаты қабылданды ма?				
А.11.4 Желіге қатынауды басқару ***Ұйым:***				
Желілік сервистерге рұқсат етілмеген қатынаудың алдын алуы тиіс.				
А.11.4.1 Пайдалануға айқын түрде рұқсат етілген сервистерге ғана қатынау пайдаланушыларға беріледі ме?				
А.11.4.2 Қашықтан пайдаланушылардың қатынауын бақылау үшін сәйкестендірудің тиісті әдістері пайдаланылады ма?				
А.11.4.3 Нақты тораптармен және жабдықпен орнатылған қосылыстардың сәйкестендіру құралдары ретінде жабдықтың автоматты сәйкестендіру ескерілді ме?				
А.11.4.4 Диагностикалық және конфигурациялық порттарға физикалық және логикалық қатынау бақыланады ма?				
А.11.4.5 Ақпараттық сервистердің, пайдаланушылардың және				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
ақпараттық жүйелердің топтарын бөлуге (оқшаулandыруға) рұқсат беретін басқару құралдары желілерде орнатылған ба?				
А.11.4.6 Ұжыммен пайдаланылатын желілер үшін (әсіресе ұйым шегінен шығатындар үшін) желіге қосылу бойынша пайдаланушылар мүмкіндіктері шектеледі ме және осы шектеулерді қолдану қатынауды басқару саясатына және бизнес-қосымшалардың талаптарына сәйкес келеді ме (А.11.1 қараңыз)?				
А.11.4.7 Компьютерлік жүйелерді қосулар және ақпараттық ағындар бизнес-қосымшалар үшін қатынауды басқару саясатын бұзбайтындығын кепілдендіруге рұқсат беретін маршруттауды басқару құралдары желілерде жүзеге асырылды ма?				
А.11.5 Операциялық жүйеге қатынауды бақылау ***Ұйым:***				
Операциялық жүйелерге рұқсат етілмеген қатынауды болдырмауға тиісті.				
А.11.5.1 Жүйеге енудің қауіпсіз процедуралары көмегімен операциялық жүйелерге қатынау бақыланады ма?				
А.11.5.2 Барлық пайдаланушыларға жеке пайдалану үшін бірегей идентификатор (пайдаланушы ИД) беріледі ме және пайдаланушының мәлімделген тұлғасын растауға рұқсат беретін аутентификацияның қолайлы әдісі таңдап алынды ма?				
А.11.5.3 Басқару жүйелері интерактивті парольдер болып табылады ма және бұл жүйелер сапалы парольдерді қамтамасыз етеді ме?				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
А.11.5.4 Қосымшаларды басқару құралдарын және жүйені өзгертуге болатын жүйелік бағдарламаларды-утилиттерді пайдалану шектелген және қатаң бақыланатын болып табылады ма?				
А.11.5.5 Әрекетсіздіктің берілген уақыты өтісімен белсендірілмеген сеанстарын жабуға рұқсат беретін басқару құралдары пайдаланылады ма?				
А.11.5.6 Жоғары тәуекелді қосымшаларды қосымша қорғауды қамтамасыз ету үшін қосу уақыты бойынша шектеулер пайдаланылады ма?				
А.11.6 Қосымшаларға және олардың ақпаратына қатынауды басқару ***Ұйым:***				
Қолданбалы жүйелерде сақталынатын ақпаратқа рұқсат етілмеген қатынаудың алдын алуға тиісті.				
А.11.6.1 Қатынауды басқарудың берілген саясатына сәйкес қолданбалы жүйелердің қызметтеріне және ақпаратқа пайдаланушылардың және қызмет көрсетуші персоналдың қатынауы шектеле ме?				
А.11.6.2 Сындарлы жүйелердің қызметі үшін бөлінген (оқшауланған) есептеуіш орта қамтамасыз етіледі ме?				
А.11.7 Мобильдік есептеу және қашықтықтан жұмыс істеу. ***Ұйым:***				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
Мобильді есептеулер және қашықтықтан жұмыс істеу құралдарын пайдалану кезінде ақпараттық қауіпсіздікті қамтамасыз етуге тиісті.				
А.11.7.1 Мобильді есептеулер және коммуникация құралдарын пайдаланумен байланысты тәуекелдерден қорғауды қамтамасыз етуге рұқсат беретін қауіпсіздіктің тиісті шаралары қабылданды ма және формальды саясат өмір сүреді ме?				
А.11.7.2 Қашықтықтан жұмыс істеу үшін саясат, оперативті жоспарлар және процедуралар әзірленіп, жүзеге асырылды ма?				
А.12 Ақпараттық жүйелерді иелікке алу, әзірлеу және ілестіру				
А.12.1 Ақпараттық жүйелердің қауіпсіздігіне қойылатын талаптар ***Ұйым:***				
Қауіпсіздік ақпараттық жүйелердің құрамдас бөлігі болып табылатындығын кепілдендіруі тиіс.				
А.12.1.1 Бизнес-талаптардың тұжырымдалуы қауіпсіздікті басқару құралдарына қойылатын талаптардың өмір сүретін ақпараттық жүйелерін модернизациялауға немесе жаңа ақпараттық жүйелерге орнатылады ма?				
А.12.2 Қосымшалардағы түзетуші өңдеу ***Ұйым:***				
Қосымшалардағы ақпараттың қателерін, жоғалуын, рұқсат етілмеген түрлендіру сын немесе тиісті түрде пайдаланылмауын болдырмауға тиісті.				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындалмайды)	
А.12.2.1 Деректердің түзетуші және дұрыс болып табылатындығын кепілдендіру үшін қосымшалардың кіру деректерінің сенімділігін тексеру жүргізіледі ме?				
А.12.2.2 Өңдеу қателерінен немесе қасақана әрекеттерден ақпараттың кез келген зақымдалуын айқындауға рұқсат беретін сенімділікті тексеру қосымшада белгіленген бе?				
А.12.2.3 Қосымшалардағы хабарламалардың тұтастығын қорғауға және аутенттілігін қамтамасыз етуге қойылатын талаптар сәйкестендірілді ме және басқарудың сәйкес құралдары сәйкестендіріліп, жүзеге асырылды ма?				
А.12.2.4 Сақталынатын ақпаратты өңдеудің түзу екендігін және ағымдағы жағдайларға сәйкес келетіндігін кепілдендіру үшін қосымшалардың шығыстық деректерінің сенімділігін тексеру орындалады ма?				
А.12.3 Криптографиялық басқару құралдары ***Ұйым:***				
Ақпараттың құпиялылығын, аутенттілігін және тұтастығын криптографиялық құралдармен қамтамасыз ету.				
А.12.3.1 Ақпаратты қорғау үшін криптографиялық басқару құралдарын пайдалану саясаты әзірленді ме және пайдаланылады ма?				
А.12.3.2 Ұйымда криптографиялық әдістерді пайдалануды қолдауға рұқсат беретін кілттерді басқару жүзеге асырылды ма?				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындал майды)**	
А.12.4 Жүйелік файлдардың қауіпсіздігі ***Ұйым:***				
Жүйелік файлдардың қауіпсіздігін қамтамасыз етуге тиісті.				
А.12.4.1 Қолданыстағы жүйелерде бағдарламалық қамтамасыз етуді орнатуды бақылау процедуралары әзірленді ме?				
А.12.4.2 Тестілік деректерді мұқият таңдау, оларды қорғау және бақылау жүзеге асырылады ма?				
А.12.4.3 Бағдарламалардың бастапқы кодына қатынау шектеледі ме?				
А.12.5 Әзірлеу және техникалық қызмет көрсету процестерінің қауіпсіздігі ***Ұйым:***				
Қолданбалы жүйелердің ақпаратын және бағдарламамен қамтамасыз ету қауіпсіздігін қолдауы тиіс.				
А.12.5.1 Өзгерістерді жүзеге асыруды бақылау үшін өзгерістерді басқарудың формальды процедуралары пайдаланылады ма?				
А.12.5.2 Қолданыстағы жүйелердің өзгеруі кезінде ұйымның қызметіне және қауіпсіздігіне жағымсыз ықпалдың жоқтығын кепілдендіру үшін бизнес үшін сыни қосымшаларды талдау және тестілеу жүргізіледі ме?				
А.12.5.3 Бағдарламамен қамтамасыз ету пакеттерін түрлендіру шектеледі ме, тек қажетті өзгертулер жүргізіледі ме және барлық өзгертулерді қатаң бақылау жүзеге асырылады ма?				
А.12.5.4 Ақпараттың жылыстауы мүмкіндіктерінің алды алынады ма?				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
А.12.5.5 Ұйым тараптық ұйымдармен бағдарламалық қамтамасыз ету әзірлемелерін бақылау және қадағалауды жүзеге асырады ма? (аутсорсинг)?				
А.12.6 Техникалық осалдықтарды басқару ***Ұйым:***				
Техникалық осалдықтар туралы жарияланған деректерді пайдаланудан туындаған тәуекелдерді азайтуы тиіс.				
А.12.6.1 Пайдалынатын ақпараттық жүйелердің техникалық осалдықтары туралы ақпаратты ұйым дер кезінде ала ма, осы осалдықтар алдында ұйымның қорғалмауы бағаланады ма, және осындай осалдықтармен байланысты тәуекелдерді жою үшін адекватты шаралар қабылданады ма?				
А.13 Ақпараттық қауіпсіздіктің оқыс оқиғаларын басқару				
А.13.1 Ақпараттық қауіпсіздік оқиғалары және қорғау әлсіздіктері жөнінде есептер құру ***Ұйым:***				
Ақпараттық жүйелермен байланысты қорғаудың әлсіздіктері және ақпараттық қауіпсіздік оқиғалары жөнінде бұл өз мезгілінде түзетуші шараларды қабылдауға рұқсат беретін түрде хабарланатындығын кепілдендіруі тиіс. .				
А.13.1.1 Тиісті басқару арналары бойынша ақпараттық қауіпсіздік оқиғалары туралы хабарлау мүмкіндігінше жылдам жүзеге асырылады ма?				
А.13.1.2 Ақпараттық жүйелерді және сервистерді пайдаланатын тараптық ұйымдардың барлық қызметкерлері, мердігерлері және				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындал майды)	
пайдаланушылары барлық бақыланған немесе болжанған жүйелерді немесе сервистерді қорғау әлсіздіктері туралы хабарлауға және белгілеуге міндетті ме?				
А.13.2 Ақпараттық қауіпсіздіктерді жетілдіруді және оқыс оқиғаларды басқару ***Ұйым:***				
Ақпараттық қауіпсіздіктің оқыс оқиғаларын басқаруға қайшы келмейтін және тиімді тәсілін қолданылатындығын кепілдендіруі тиіс.				
А.13.2.1 Ақпараттық қауіпсіздіктің оқыс оқиғаларына жылдам, тиімді және дұрыс әрекет етуді қамтамасыз ететін процедуралар және басшылық жауапкершілігі белгіленді ме?				
А.13.2.2 Ақпараттық қауіпсіздіктің оқыс оқиғаларының типтерін, көлемдерін және құнын өлшеуге және қадағалауға рұқсат беретін механизмдер жүзеге асырылды ма?				
А.13.2.3 Егер ақпараттық қауіпсіздіктің оқыс оқиғалары нәтижесінде тұлғаға немесе ұйымға қатысты қабылдау шамаланатын әрекеттер құқықтық әрекеттерді (азаматтық, сондай-ақ қылмыстық кодекс бойынша) қамтитын болса, онда сәйкес құқық қорғау органында (органдарында) белгіленген дәлелдер ережелеріне сәйкес дәлелдерді жинау, сақтау және беру жүзеге асырылады ма?				
А.14 Бизнестің үздіксіздігін басқару				
А.14.1 Бизнестің үздіксіздігін басқарудағы ақпараттық қауіпсіздік аспектілері				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
***Ұйым*:**				
Бизнес-қызметтегі іркілістерге қарсы әрекет етуге және сындарлы бизнес-процестерді ақпараттық жүйелердің ірі апаттарының немесе катастрофалардың салдарынан қорғауды қамтамасыз етуге, сонымен қатар жұмыстың дер кезінде қалпына келтірілуін қамтамасыз етуге тиісті.				
А.14.1.1Аталмыш ұйым бизнесінің үздіксіздігі үшін қажетті ақпараттық қауіпсіздік талаптарын ескеретін ұйым шеңберінде бизнестің үздіксіздігін қамтамасыз етудің басқарылатын процесі әзірленді ме және қолдау көрсетіле ме?				
А.14.1.2 Бизнес-процесстер тоқтатылуы мүмкін барлық оқиғалар сәйкестендірілді ме және осындай тоқтаулардың ықтималдығы және ықпалы және ақпараттық қауіпсіздікке әсері анықталды ма?				
А.14.1.3 Операцияларды қолдауға немесе қалпына келтіруге, сонымен қатар сындарлы бизнес-процестердің тоқтауынан немесе іркілісінен кейін талап етілетін деңгейде және талап етілетін уақытта ақпараттың қолжетімділігін қамтамасыз етуге рұқсат беретін жоспарлар әзірленіп, жүзеге асырылды ма?				
А.14.1.4 Барлық жоспарлардың қарама-қайшылықсыздығын, ақпараттық қауіпсіздік талаптарының тұрақты есебін және тестілеу және ілестіру үшін басымдылықтарды анықтауды кепілдендіруге рұқсат беретін, бизнестің үздіксіздігін қамтамасыз ету жоспарларының бірегей құрылымына қолдау көрсетіледі ме?				
А.14.1.5 Бизнестің үздіксіздігін қамтамасыз ету жоспарларын,				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
олардың өзектілігін және тиімділігін кепілдендіру үшін тұрақты тексеру және жаңғырту жүргізіледі ме?				
А.15 Формальды талаптарға сәйкестік				
А.15.1 Құқықтық талаптарға сәйкестік ***Ұйым:***				
Міндеттемелер, регулятивті немесе шарттық міндеттемелер заңына негізделген заңдардың, сонымен қатар барлық қауіпсіздік талаптарының бұзылуынан сақтауы тиіс.				
А.15.1.1 Әрбір ақпараттық жүйе және ұйым үшін барлық заң талаптары, регулятивті және шарттық талаптар, сонымен қатар осы талаптарды қанағаттандыру үшін пайдаланылатын ұйым әдістемесі айқын анықталып, құжатталды ма және өзекті күйде ұсталынады ма?				
А.15.1.2 Зияткерлік меншік құқықтары тарайтын материалдарды пайдалану бойынша, сонымен қатар патенттелген бағдарламалық өнімдерді пайдалану бойынша құқықтық, регулятивтік және шарттық талаптарға сәйкестікті кепілдендіретін тиісті процедуралар жүзеге асырылды ма?				
А.15.1.3 Маңызды жазбаларды заң талаптарына, регулятивтік және шарттық талаптарға, сонымен қатар бизнес-талаптарға сәйкес жоғалудан, жойылудан және қолдан жасаудан қорғау жүзеге асырылады ма?				
А.15.1.4 Деректердің қорғалуын және құпиялылығын сәйкес заңнама талаптарына, регулятивтік ережелерге және қолданған жағдайда				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	**ІШІНАРА (ішінара орындалады)**	**ЖОҚ (орындалмайды)**	
шарттардың ережелеріне сәйкес қорғалуын және құпиялылығын қамтамасыз ететін басқару құралдары қолданылады ма?				
А.15.1.5 Ақпаратты өңдеу құралдарын рұқсат етілмеген мақсаттар үшін қолданудан пайдаланушыларды тоқтатын шаралар қабылданады ма?				
А.15.1.6 Криптографиялық басқару құралдарын пайдалану барлық релевантты келісімдерге, заңдарға және регулятивті ережелерге сәйкес келеді ме?				
А.15.2 Стандарттарға және қауіпсіздік саясаттарына сәйкестік, техникалық сәйкестік ***Ұйым:***				
Ұйымда қабылданған жүйелердің қауіпсіздік стандарттарына және саясаттарына сәйкестігін қамтамасыз етуге тиісті.				
А.15.2.1 Менеджерлер өздерінің жауапкершілігі шегінде қауіпсіздік стандарттарына және саясаттарына сәйкестікті кепілдендіру үшін барлық қауіпсіздік процедураларының түзу орындалуын қамтамасыз етуге арналған шаралар қабылдай ма?				
А.15.2.2Қауіпсіздікті қамтамасыз ету стандарттарына сәйкестікке ақпараттық жүйелердің тұрақты тексерілуі орындалады ма?				
А.15.3 Ақпараттық жүйелердің аудитін талдау ***Ұйым:***				
Бір жақтан аудит процесінің ақпараттық жүйелерге, екінші жағынан – аудит процесіне ақпараттық жүйелердің әсерін төмендетуі және аудит процесінің тиімділігін арттыруы тиіс.				

Тексерілетін стандарт талабы	Стандарт талабының орындалуын бағалау			Стандарт талабын орындау бойынша нұсқаулар
	ИӘ (толығымен орындалады)	ІШІНАРА (ішінара орындалады)	ЖОҚ (орындал майды)	
А.15.3.1 Бизнес-процестерде іркіліс тәуекелін азайту үшін өндірістік жүйелерді тексеруді қамтитын қызмет және аудит талаптарын мұқият жоспарлау және сәйкестендіру орындалады ма?				
А.15.3.2 Кез келген мүмкін болатын тиісті емес пайдалануды немесе беделіне нұқсан келтіруді болдырмау мақсатында ақпараттық жүйелер аудитының құралдарына қатынауды қорғау іске асырылады ма?				

6 *ҚР СТ ИСО/МЭК 27001* стандартымен қарастырылған басқару құралдарының және мақсаттарының аудиті

6.1 Қауіпсіздік саясаты

6.1.1 Ақпараттық қауіпсіздік саясаты

Мақсат: мақсатты тұжырымдау және ұйым басшылығымен ақпараттық қауіпсіздікті қолдауды қамтамасыз ету.

6.1.1.1 Ақпараттық саясат туралы құжат

Қауіпсіздік саясаты туралы жазбаша құжат ұйым басшылығымен бекітілуі, жариялануы және барлық қызметкерлердің назарына жеткізілуі тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Аталмыш саясат артық нақтылыққа берілмеуі тиіс, бірақ онда ақпараттық қауіпсіздікті қамтамасыз етуге басшылықтың ұмтылысы айқын белгіленуі тиіс, ол бойынша өзгерістердің есебі жүргізілуі тиіс, ал құжатта жауапты басшы тұлғаның қолы болуы тиіс. Саясат ең аз дегенде келесі мәліметтерді қамтуы тиіс:

– Ақпараттық қауіпсіздікті анықтау,

– Ақпараттық қауіпсіздік ұйым үшін маңызды болып табылатын себептер; ақпараттық қауіпсіздіктің қағидаттары мен мақсаттары,

– Қауіпсіздік саясаттары, стандарттары және сәйкестік бойынша талаптар туралы қысқа мәліметтер,

– Ақпараттық қауіпсіздікті қамтамасыз ету бойынша барлық релевантты міндеттерді анықтау.

– Сәйкес қосымша құжаттарға сілтемелер.

Аудитор саясатқа кез келген қызметкердің жеңіл қол жеткізе алатындығына, барлық қызметкерлер оның барлығы жөнінде хабардар болуына және оның мағынасын түсінетіндігіне көз жеткізуі керек. Саясат жеке құжат болып табылады не ақпараттық қауіпсіздік саясаты ұйымға қандай түрде енгізілетіндігін анықтайтын неғұрлым толық құжаттама пакетінің құрамына кіруі мүмкін (мысалы, қауіпсіздік саясаты бойынша Нұсқаулық). Қызметкерлердің барлығы болмаса да, көбіне АҚБЖ қолдану аясына жатқызылмайтын көпшілігі ақпараттық қауіпсіздік саласында белгілі бір міндеттемелерге ие болады, аудиторлар осы деректі жоққа шығаратын кез келген мәлімдемеге абайлап қарауы тиіс.

Оның үстіне, аудитор саясат үшін оны қолдауға жауапты тұлға анықталғандығына, ал саясаттың өзі тәуекелдердің бағалануы жүргізілген мәселелерді қозғайтын кез келген өзгерістерге сәйкес жаңғыртылып отыратындығына көз жеткізуі тиіс.

6.1.1.2 Қайта қарау және талдау

Саясат тұрақты, ал елеулі өзгертулер жағдайында оның адекваттығын сақтау мақсатында қайта қаралуы және талдануы тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Аталмыш басқару құралы ақпараттық қауіпсіздік саясатының өзектілігін және тиімділігін қамтамасыз ету үшін қажет. Бұл саясат АҚБЖ құру және қолдау кезінде маңызды роль ойнайды. Аудиторлар ұйымда кез келген оқыс оқиғаларға, жаңа осалдықтарға және қауіпсіздік қатерлеріне, техникалық өзгерістерге және АҚБЖ-ға қатысы бар қалғандардың барлығына әрекет ету процедуралары әзірленгендігіне көз жеткізуі қажет және саясатты қайта бағалауды талап ете алады. Оның үстіне, ұйымда саясаттың өзекті екендігіне, ал оны енгізу ұсынылатын қорғау деңгейіне қатысты экономикалық тұрғыдан ақталғандығына көз жеткізу үшін саясатты кезеңді түрде қайта қарау жоспарлануы тиіс. Аудитор саясатты қайта қарау графигі тәуекелдер бойынша жалпы жағдайға сәйкес келетіндігіне көз жеткізуі қажет. Аудиторлар сонымен қатар саясаттың жаңартылған нұсқаларын тарату бойынша ұйым жоспарларын тексеруі және барлық қызметкерлерге енгізілген өзгертулер туралы ақпарат жеткізілгендігіне көз жеткізуі тиіс.

6.2 Қауіпсіздікті қамтамасыз ету

6.2.1 Ақпараттық қауіпсіздіктің инфрақұрылымы

Мақсат: Ұйымдағы ақпараттық қауіпсіздікті басқару.

Ақпараттық қауіпсіздік саясатын бекітуді, қауіпсіздікті қамтамасыз ету бойынша міндеттерді бөлуді және ұйым шегінде қауіпсіздікті енгізуді үйлестіру үшін жоғарғы басшылықпен сәйкес мәслихаттар өткізілуі тиіс. Қажет болса, мамандардан ақпараттық қауіпсіздік бойынша кеңестер және мәліметтер алу тәсілдерін ескеруі және ұйым шегінде осындай ақпаратқа қолжетімділікті қамтамасыз етуі керек. Аталмыш салада ағымдық үрдістерді, стандарттарды және бағалау әдістерін қадағалау үшін қауіпсіздік бойынша сыртқы мамандармен қатынастарды, сонымен қатар қауіпсіздіктің оқыс оқиғаларымен жұмыс істеу кезінде осындай мамандармен тиісті байланысу тәсілдерін өңдеуді жолға қою және ұстану керек. Ақпараттық қауіпсіздікке дисциплина аралық әдістемені ынталандыру қажет, мысалы, сақтандыру және тәуекелдерді басқару секілді салаларда қауіпсіздік бойынша мамандардың, аудиторлардың, қосымшаларды әзірлеушілердің, әкімгерлердің, пайдаланушылардың және менеджерлердің ынтымақтастығы.

6.2.1.1 Ақпаратты қорғау проблемалары бойынша басшылық мәслихаты және ақпаратты қорғау бойынша әрекеттерді үйлестіру

Ұйым басшылығы нақты нұсқауларды әзірлеу және қауіпсіздікті қамтамасыз ету бойынша бастамаларды әкімшілік қолдауды қамтамасыз ету

үшін мәслихаттарды тұрақты өткізуі тиіс. Басшылық мәслихаттары қажетті қатысу және ресурстарды жеткілікті бөлу арқылы қауіпсіздікті қамтамасыз етуге атсалысуы тиіс.

Ірі ұйымдарда ақпараттық қауіпсіздікті басқару құралдарын жүзеге асыру бойынша әрекеттерді үйлестіру мақсатында әртүрлі бөлімшелер басшыларының қатысуымен маслихаттар өткізілуі тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Бұл тетік қауіпсіздік саласындағы ұйым қажеттіліктерін сәйкестендіру, сонымен қатар олардың балама қанағаттандырылуын және кезеңдік қайта қарауын қамтамасыз ету үшін қажетті. Бұл топтың АҚБЖ құру және қолдау үшін жауапты болатындығы болжанады. Мәслихат қатысушылары сәйкес өкілеттіктерге ие болуы тиіс, сондықтан аудиторлар оның ақпараттық қауіпсіздікке жауапты тұлғаның басшылығымен немесе ең аз дегенде қатысуымен өткізілуіне көз жеткізуі тиіс. Отырыс хаттамасы формальды түрде белгіленуі тиіс; жүргізілуі жөнінде шешім қабылданған кез келген әрекеттер айқын анықталған процедуралар көмегімен қадағалануы тиіс. Мәслихатты өткізуге прагматикалық әдістеме қажет; шағын ұйымдар үшін ақпараттық қауіпсіздік бойынша мәслихаттарды өткізуді басқа шаралармен үйлестіру мақсатқа сай болуы мүмкін, алайда бұл жағдайда ақпараттық қауіпсіздік мәселелерін балама айқындауды қамтамасыз ету және хаттамада қауіпсіздікке қатысты проблемалардың анық белгіленгендігін қадағалау қажет.

Ірі ұйымдар, сонымен қатар ақпараттық қауіпсіздікке қоятын талаптары жоғары ұйымдар қауіпсіздік мәселелерін талқылауға жеке мәслихат арнауы тиіс. Аудитор бұл мәслихаттардың, сонымен қатар қауіпсіздік саясатын қайта қарау секілді басқа шаралардың жеткілікті мерзімділікпен өткізілетініне көз жеткізуі қажет. Мәслихат қатысушыларының саны және құрамы нақты ұйымның талаптарымен анықталады. Мысалы, шағын ұйымда, мәслихатқа тек атқарушы директор және ақпараттық қауіпсіздікке жауапты тұлға қатысуы мүмкін, ал ірі концерндер үшін әрбір бөлімше өкілдерінің, қауіпсіздік бойынша қызметкерлердің және жоғарғы басшылықтың қатысуымен кеңейтілген мәслихат форматы қисынды. Аудитор нақты ұйымның қажеттіліктерінен және АҚБЖ мәлімделген масштабынан шығара келе әрбір жағдайды бағалауы тиіс. Технологияның заманауи даму қарқындарын, ақпаратты өңдеу құралдарын пайдаланатын ұйымдарды ескере отырып, қауіпсіздікті қамтамасыз ету бойынша процедураларды ең аз дегенде алты айда бір рет қайта қарау қажет.

6.2.1.2 Ақпараттық қауіпсіздікті қамтамасыз ету бойынша міндеттерді бөлу

Жеке ресурстарды қорғау және қауіпсіздікті қамтамасыз етудің нақты процестерінің орындалуы бойынша міндеттер анық анықталуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Аудиторлар барлық деңгейлердегі міндеттердің анық анықталғандығына көз жеткізуі қажет. Міндеттер туралы хабардар болушылық және персоналдың жауапкершілікті қабылдауы сәйкес куәліктермен расталуы тиіс. Жауапкершілікті және есептіліктің құрамын неғұрлым жоғары деңгейде анықтау үшін әдетте қауіпсіздік саясаты және/немесе тәуекелдерді өңдеу жоспары пайдаланылады, алайда ақпараттық қауіпсіздік үшін жауапкершіліктің нақты аспектілері нақты жағдайға байланысты көбіне лауазымдық міндеттерді сипаттауға енгізіледі, не басқа форматта көрсетіледі. Әрбір ресурс бойынша оның қауіпсіздігін қамтамасыз ету үшін жауапты тұлғаны анықтау мүмкіндігі болуы қажет. Аудиторлар ұйымда тұтас алғанда ақпараттық қауіпсіздік үшін жауапты тұлға тағайындалуына (мысалы, ақпараттық қауіпсіздік жөніндегі жетекші), ал барлық жауапты қызметкерлер ақпараттық қауіпсіздікті қамтамасыз ету бойынша өз міндеттері жөнінде хабардар болғандығына көз жеткізуі керек. Аудиторлар сонымен қатар барлық сәйкес құжаттаманың ағымдағы сәтте өзекті болып табылатындығын және оны жаңғырту тиісті түрде бақыланатындығын тексеруі тиіс.

6.2.1.3 Ақпараттық жүйелерді бекіту процесі

Жаңа ақпараттық жүйелерді басшылықпен бекіту процедурасы анықталуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Қауіпсіздікті басқару құралдарының тұтастығын қадағалау өте маңызды. Соған сәйкес, ақпараттық жүйелерді іріктеудің кеңеюі не өзгеруі басшылық тарапынан тиісті түрде бақылануы тиіс. Бекіту және рұқсат алу процедуралары анық тұжырымдалуы және жүзеге асырылуы, сонымен қатар сәйкес құжаттамамен расталуы тиіс. Аудиторлар жаңа бағдарламалық құралдарды орнату, нұсқаларды жаңарту, баптауларды өзгерту, сонымен қатар қауіпсіздік инфрақұрылымын қозғайтын кез келген басқа процедуралар ұйым басшылығымен сәйкес деңгейде мақұлданғандығына, техникалық тұрғыдан тексерілгеніне, баптауларды өзгерту жоспарында қадағалануына және тиісті түрде құжатталғанына көз жеткізуі қажет. Жаңа жүйелерді енгізу және оларды қызметкерлердің өндірістік мақсаттарда пайдалану айқын түрде басшылықпен рұқсат етілуі тиіс.

6.2.1.4 Ақпараттық қауіпсіздік бойынша мамандардың ұсыныстары

Ұйым ақпараттық қауіпсіздікті қамтамасыз ету бойынша ұсыныстар алу үшін меншікті немесе сыртқы консультанттарға хабарласуы тиіс және алынған ұсыныстарды барлық ұйым аясында үйлестіруі тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Ақпараттық қауіпсіздік мәселелері бойынша кеңестерге қашан және қандай көлемде жүгіну мәселесі тұтастай нақты ұйым құзыретіне

жатқызылады. Бір жағдайда ұйым ішінде ақпараттық қауіпсіздік бойынша консультанттарды немесе мәліметтердің басқа көзін іздеу, ал басқа жағдайда – аталмыш салада танымал сарапшылар немесе кәсіби консультанттар секілді тараптық мамандардың немесе ұйымдардың көмегіне жүгіну, ал үшінші жағдайда – құрамалы әдістемені пайдалану мақсатқа сай болады. Таңдап алынған әдістемеге тәуелсіз қауіпсіздік бойынша мәслихаттармен анық байланыс ұсталуы тиіс. Аудитор қандай қосымша мәліметтер берілетіндігін, олардың адекватты жағдайлар болып табылатындығын, ақпарат көзінің жеткілікті түрде біліктілігін көтеруін анықтауы, сонымен қатар консультация анық талап етілетін, бірақ оларға сұраныс түспеген салаларды айқындауы керек. Бұл жағдайда қауіпсіздікті басқару құралдарына қолжетімділік тиісті түрде басшылықпен авторландыруы тиіс, ал қажет болса жабдықты жеткізушімен қосымша бақылануы тиіс. Сонымен қатар қауіпсіздіктің оқыс оқиғалары бойынша есептерді талдауға ұсыныс беріледі: тағайындалған мамандар оқыс оқиғаның себептерін бағалауға қатысады ма, ұсынылған түзетуші шаралар жүргізілді ме? Шағын ұйымдарда қауіпсіздік бойынша жауапты маман (немесе баламалы лауазымдағы қызметкер) ақпараттық қауіпсіздік бойынша мәліметтердің жалғыз дереккөзі болуы мүмкін. Бұл жағдайда аудиторлар бұның қауіпсіздік бойынша бар талаптарды қанағаттандыру үшін жеткілікті екендігіне, ұйымда технология және қауіпсіздік саласында өзгертулердің қадағалануына, ал қажет болса консультация үшін сыртқы ресурстар тартылатындығына көз жеткізуі қажет.

6.2.1.5 Ұйымдар арасындағы ынтымақтастық

Құқық қорғау органдарымен, бақылау органдарымен, ақпараттық қызметтерді жеткізушілермен және байланыс қызметтерінің операторларымен қажетті байланыстар ұсталуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Басқарудың аталмыш құралы қауіпсіздіктің оқыс оқиғаларының алдын алу немесе осындай оқыс оқиғалардың салдарларын азайту кезінде елеулі роль ойнауы мүмкін сыртқы бақылау органдарымен, қызметтерді жеткізушілермен және басқа ұйымдармен байланыс каналдарының болуын талап етеді. Соған сәйкес, аудитор төтенше жағдайларда әрекеттерді жоспарлаумен және инфрақұрылымды қолдаумен шұғылданатын қажетті байланысу тұлғаларының болуын анықтауды талап етеді. Аудитор ұйымда құқықтық саладағы талаптардың, сонымен қатар өндірістік жоспардағы операциялық және техникалық талаптардың қадағалануына және осындай талаптарға сәйкестікті қамтамасыз ететіндігіне куәлік табуы қажет. Аудитор ұйымда жағдайға қатысты қолданылатын барлық заңнамалық талаптардың белгілі екендігіне, бұл талаптардың құжатталуына және талаптарды орындау үшін қажетті барлық қатынастардың жолға қойылғандығына көз жеткізуі керек.

Оның үстіне, ұйым үшін алдыңғы қатарлы тәжірибелерді таратуға қатысу және өз саласындағы тараған қатерлер жөніндегі ақпаратпен алмасу пайдалы. Ірі ұйымдар қауіпсіздік бойынша мамандандырылған топтардың, стандарттарды қабылдау жөніндегі комитеттердің жұмысына және осындай тектес басқа өндірістен тыс шараларға қатыса алады. Шағын ұйымдар осындай шараларға белсенді қатысу мүмкіндігіне ие болмауы мүмкін, бірақ пішінді конференцияларға және семинарларға қатысып тұру бұл деректі ішінара өтеуі мүмкін.

6.2.1.6 Ақпараттық қауіпсіздікті тәуелсіз талдау

Ақпараттық қауіпсіздік саясатын жүзеге асырудың тәуелсіз талдауы жүргізілуі тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Аудитор үшін кезеңдік талдаудың шын мәнінде жүргізілетіндігіне және тәуелсіз тұлғалармен орындалатындығына көз жеткізу маңызды. Тәуелсіз талдауды жүргізбей толық объективтілікті кепілдендіру мүмкін емес. Тараптық мамандармен жүргізілетін аудит жоғарыда келтірілген талаптарды қанағаттандырады. Тараптық аудит жүргізілмеген жағдайларда талдау ішкі аудиторлар, басшылық немесе ақпараттық қауіпсіздікті қамтамасыз етуші қызметкерлерден бөлек жұмыс істейтін басқа тұлғалармен жүргізілуі мүмкін. Сонымен қатар ақпараттық жүйелердің қауіпсіздігін Тексеру секілді басқа тексерулердің нәтижелерін ескеру қажет (6.10.2-қара).

6.2.2 Тараптық ұйымдардың қатынау қауіпсіздігі

Мақсат: тараптық ұйымдар қатынауға ие ұйымның ақпараттық ресурстарының қауіпсіздігін қамтамасыз ету.

6.2.2.1 Тараптық ұйымдардың қатынауымен байланысты тәуекелдерді сәйкестендіру

Тараптық ұйымдардың ұйымның ақпараттық ресурстарына қатынауымен байланысты тәуекелдерді бағалау орындалуы тиіс және қауіпсіздікті басқарудың сәйкес құралдары жүзеге асырылуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Бірінші кезекте аудитор ақпараттық ресурстарға үшінші мекеменің/тұлғаның қатынауымен байланысты тәуекелдерді айқындау үшін ұйыммен орындалатын бағалауды тексеруі қажет. Тәуекелдер Интернет немесе таяу қаралымда, әсіресе қашықтағы бөлімшелер арасындағы жұмыс кезінде әлдеқайда аз оқшауландырылған болып көрінетін Интранет арқылы қосылыстарды пайдаланумен есептегіш торапқа немесе серверлік бағдарламамен қамтамасыз етуге қашықтан қатынаумен байланысты болуы мүмкін. Байланыс АҚБЖ формальды қамтымаған бөлімшелерден орнатылуы әбден мүмкіндігін есте сақтау керек. Сонымен қатар тараптық ұйыммен ақпараттық қауіпсіздік тұтастығын бағалау үшін қандай шаралар

қабылданатындығын, басқару құралдары қорғаудың жеткілікті дәрежесін қамтамасыз ететіндігін және тәуекелдерді қайта бағалау қаншалықты жиі жүретіндігін талдау қажет.

6.2.2.2 Тараптық ұйымдармен жасалған келісім-шарттардағы қауіпсіздік шарттары

Тараптық ұйымдардың ұйымның ақпараттық ресурстарына қатынауын қарастыратын келісімдер формалды келісім-шартта негізделуі тиіс, онда барлық қажетті қауіпсіздік шарттары аталуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Аудитор тараптық ұйымдармен іс жүргізу кезіндегі қауіпсіздік бойынша барлық талаптардың сәйкестендірілуін және екі ұйым арасында жасалған қызметтерді беру туралы келісімге немесе формальды шартқа енгізілуіне көз жеткізуі қажет.

6.2.3 Аутсорсинг

Мақсат: Ақпаратты өңдеу жауапкершілігі аутсорсинг келісім-шартына сәйкес басқа ұйымға табысталатын жағдайларда ақпараттың қауіпсіздігін қамтамасыз ету

6.2.3.1 Аутсорсинг келісім-шарттарындағы қауіпсіздік шарттары

Тараптар арасында жасалған келісім-шартта ақпараттық жүйелерінің, желілерінің және/немесе үстелдік жүйелер орталарының барлығына немесе кейбіріне бақылауды және басқаруды беретін ұйым қауіпсіздігі шарттары ескерілуі тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Ақпаратты өңдеу бойынша міндеттерді аутсорсингке табыстау қауіпсіздік жоспарында тәуекелдің белгілі бір деңгейін қамтиды, өйткені ұйым аталмыш міндеттерге тікелей бақылауды жоғалтады. Аутсорсингпен байланысты тәуекелдерден қорғау тәсілдерінің бірі келісім-шартты жасау болып табылады, онда қауіпсіздік бойынша талаптар, басқару құралдары және қос тараптың жауапкершілігі анық анықталған. Аудиторлар ұйымдағы қауіпсіздік бойынша барлық талаптарды жабатын келісім-шарттың болуына көз жеткізуі қажет. Келісім-шарттың нақты мазмұны тәуекелдерді бағалау негізінде анықталады.

6.3 Ресурстарды жіктеу және оларды бақылау

6.3.1 Ресурстар үшін жауапкершілік

Мақсат: ұйым ресурстарының тиісті қорғалуын қамтамасыз ету.

6.3.1.1 Ресурстарды түгендеу

Әрбір ақпараттық жүйемен байланысты барлық маңызды ресурстардың тізімдемесі құрылуы тиіс және өзекті күйде ұсталуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Ұйымдарға ресурстардың дәл тізімдемесіне ие болу және оны өзекті күйде ұстау қажет. Тізімдемеге қорғауға жататын барлық негізгі ақпараттық және физикалық ресурстар, бағдарламамен қамтамасыз ету, сервистер және процестер енгізілуі тиіс. Тексеру барысында бірінші кезекте ресурстардың тиісті түрде сәйкестендірілуіне және жіктелуіне көз жеткізу қажет. Аудитор тізімдеменің күйін бағалауы керек: оның толықтығы және дәлдігі, барлық қажетті ақпараттың, жаңарту күні мен әдістемесінің болуы, жабдықты табыстау туралы жазбалардың болуы.

Ресурстардың түгенделуіне жауапты тұлғаның барлығына көз жеткізу қажет. Сонымен қатар түгендеу тізімдеме қандай түрде қорғалғандығын тексеру қажет: егер түгендеу тізімдеме электронды түрде жүретін болса, қатынау қалай бақыланады және резервтік көшірмелер бар ма, егер қағаз түрінде жүрсе – құжаттар қайда сақталынады, олар жоғалып қалудан қалай қорғалған, егер жазбаны ауыстыру қажет болса не істейді, ескі даналар сақталынады ма және егер сақталынса, онда олар қай мерзімге дейін және қайда сақталынады... Ресурстардың түгендеу тізімдемесі анық сәйкестендірілуі тиіс:

– бірегей сериялық нөмірді, күнді және т.с.с. (қолданылатын жерде) көрсетумен нысан;

– қауіпсіздік класы;

– иегер;

– орналасқан жер;

– тасымалдаушы (ақпараттық ресурстар үшін);

– тізімдемеге енгізу және/немесе аудиторлық тексеру күні.

6.3.2 Ақпаратты жіктеу

Мақсат: Ақпараттық ресурстардың тиесілі қорғау деңгейін қамтамасыз ету.

6.3.2.1 Жіктеу бойынша ұсыныстар

Ақпарат санаттары және олармен байланысты ақпаратты басқаруды қорғау құралдары ақпаратты ұжымдық пайдалануға немесе оған қатынауды шектеуге өндірістік қажеттілікті, сонымен қатар осындай қажеттілікпен байланысты ұйымға әсерді ескеруі тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Аудиторлар ұйымның жіктеудің балама қағидаттарын әзірлеу және жүзеге асыру үшін жеткілікті күш салғандығын растауы тиіс. Ресурстарды қалыпты қорғау үшін құпиялылық, тұтастылық және қолжетімділік секілді осындай негізгі сәттерді жеткілікті деңгейде көрсететін градацияның немесе жіктеудің кейбір формалары болуы қажет. Жіктеу сызбасы АҚБЖ қолдану

аясына түсетін барлық ресурстарға қолданылуы тиіс. Жіктеудің анық жүйесінсіз ресурстардың адекватты қорғалуын қамтамасыз ету мүмкін емес.

Осындай сызба өте күрделі болмауы тиіс және жіктеу сызбаларда ықтимал айырмашылықтарды түсінуді қамтамасыз етуге рұқсат беретін басқа ұйымдармен жасалған келісімдермен бекітілуі тиіс. Процедуралар жіктеу дұрыстығын тексеруді қарастырады ма? Жіктеу деңгейін төмендету процедурасы өмір сүреді ме? Жіктеу сызбасына оңай қол жеткізуге болатындығына, қызметкерлердің оның болуы жөнінде хабардар етілгендігіне және жіктеу қағидаттарын түсінетіндігіне, ал сызбаның ұдайы жаңғыртылып отыратындығына көз жеткізіңіз. Нақты ресурс жіктелуі үшін жауапкершілікті оның иегері көтереді.

6.3.2.2 Ақпаратты өңдеу және таңбалау

Ұйымда қабылданған жіктеу сызбасына сәйкес ақпаратты өңдеу және таңбалау үшін процедуралар анықталуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Ұйымдарда қабылданған жіктеу сызбасына сәйкес жіктелген ақпаратпен жұмыс істеудің және таңбалаудың процедуралары қарастырылуы тиіс. Аудиторлар сонымен қатар сәйкес таңбалаумен осал ақпараттық бірлік (мысалы, ақпаратты немесе деректер базасын өңдеу жүйесі) бөлінгендігіне көз жеткізуі керек.

Құжаттама, үлдірлер, аппараттық құралдар және т.с.с. секілді шынайы нысандардың таңбалауы тривиалды мардымсыз міндет болып табылады, алайда электронды түрде берілетін ақпаратпен және хат-хабармен не істеу керек? Электронды түрдегі ақпаратты таңбалау үшін ұйыммен таңдап алынған шешімдер адекватты екендігіне көз жеткізу қажет: таңбалау процедураларының анық және түсінікті сипаттамасы бар ма, ақпаратты алушы категория атауын дұрыс түсінеді ме, таңбалау ақпаратты пайдалану және сақтау кезінде оның тиісті түрдегі қорғалуына атсалыса ма. Физикалық ресурстар дұрыс таңбаланған ба? Кейбір жағдайларда инвентарлы құлақшалар сәтсіз орналастырылуы және дереу белгілі болмауы мүмкін; жапсырмалардың желімдері затты таңбалаусыз және стандартты қорғаусыз қалдырып, ажыратылуы мүмкін.

6.4 Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметкерлермен жұмыс

6.4.1 Лауазымдық нұсқаулардағы және ресурстарды бөлу кезіндегі қауіпсіздік

Мақсат: Персоналдың қателесуі, алаяқтық немесе жабдықты дұрыс пайдаланбау тәуекелдерін азайту.

6.4.1.1 Лауазымдық нұсқаулықтардағы қауіпсіздік

Ұйымда қабылданған ақпараттық қауіпсіздік саясатымен орнатылған қауіпсіздікті қамтамасыз ету үшін жауапкершілік және міндеттер лауазымдық нұсқаулыққа енгізілуі тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Ақпараттық қауіпсіздіктің нақты мәселелері үшін жауапкершілік көтеретін барлық қызметкерлерде қауіпсіздік қамтамасыз етуге жауапкершілікті және нақты міндеттерді анықтайтын лауазымдық нұсқаулықтар не оларға балама құжаттар болуы тиіс. Аудиторлар осындай нұсқаулықтардың барлығына, түсіну және міндеттерді қабылдау қызметкердің өзінің және оның жетекшісінің қолымен расталуына, құжатта күн қойылып, ал қауіпсіздіктің сәйкес мәселелері онда анық және бірізділікпен берілгендігіне көз жеткізуі тиіс. Жеке процедураларды сипаттау және саясат құжаттарында белгіленген қауіпсіздік бойынша міндеттерді тексеру лауазымдық нұсқаулықтарына толық сәйкестікті көрсетуі тиіс.

Әртүрлі ұйымдарда лауазымдық нұсқаулықтарды сақтау тәжірибелері ерекшеленуі мүмкін. Бір ұйымдарда осындай нұсқаулықтар тікелей қызметкерге беріледі, ал басқаларында нұсқаулықтар кадр бөлімінде сақталынады. Соңғы жағдайда қызметкердің аталмыш ақпаратқа қолжеткізе алатындығына көз жеткізу керек – қызметкерде лауазымдық нұсқаулықтың меншікті данасы болуы тиіс, өйткені адам соңғы рет, бір жылдан көп уақыт бұрын көруі мүмкін құжаттың жазбаша өкімін қадағалайтындығы екіталай. Егер қызметкердің лауазымы қауіпсіздікті қамтамасыз ету бойынша нақты міндеттерді білдіретін болса (мысалы, жүйелік әкімгерлер), оның тиісті түрде лауазымдық міндеттерінде көрсетілгендігіне көз жеткізіңіз; барлық қызметкерлерге қатысты стандартты тұжырымдаулар осындай жағдайда қолданылмайды. Сонымен қатар ескірген сипаттауларға, мысалы, егер қызметкер осы сәтте басқа жұмысты орындаған жағдайда жол берілмейді.

Әсіресе, жаңа қызметкерлердің өз міндеттерін және олармен байланысты жауапкершілікті толықтай түсінуі маңызды; сәйкес құжаттар постфактум емес, қызметке тағайындау кезінде рәсімделуі тиіс. Аудиторлар келісім-шарт бойынша жұмыс істейтін персонал және уақытша қызметкерлерге ерекше назар аударуы керек, өйткені оларда ресми рәсімделген лауазымдық нұсқаулықтар болмауы мүмкін. Мұндай жағдайға жол берілмейді; лауазымдық нұсқаулармен АҚБЖ қолдану саласына тартылған барлық персоналды қамтамасыз ету керек.

Кем дегенде барлық қызметкерлердің құпиялылықты қадағалау туралы шартқа (төменде қараңыз) қол қоюына, ал оның қызметтері келісім-шартта көрсетілгендігіне көз жеткізу керек. Тиісті нұсқаулықтарға енгізілген қауіпсіздік мәселелерін мұқият талдау керек, өйткені нақ осында әлеуетті «әлсіз буын» болуы мүмкін.

5.4.1.2 Жұмысқа қабылдаушыларды тексеру

Жұмысқа қабылдау туралы арыздарды қарау кезінде тұрақты персонал, келісім-шарт бойынша жұмыс істейтін қызметкерлер және уақытша персонал үшін берілген мәліметтердің сенімділігі тексерілуі тиіс.

Аудит жүргізу жөніндегі нұсқаулық:

Персоналды іріктеу процедуралары (келісім-шарт бойынша жұмыс істейтіндерді және уақытша персоналды қоса) берілген мәліметтердің сенімділігін тексеру әдістемесін қосуы тиіс. *ҚР СТ ИСО/МЭК* 17799 стандартында қарауға арналған сұрақтардың тізімі келтіріледі; соның ішінде, ұйымдар тиісті тексерулер жүргізбей, жалғыз резюме негізінде берілген мәліметтерді сенімді деп санамауы керек. Жұмысқа қабылдау үшін жауапты тұлғамен талқылау секілді кез келген кейінгі әрекеттер құжатта белгіленуі тиіс. Жетекшілер өздерінің құзыреттілігі аясында ұйымда жүргізілетін жұмыстарды талдау және бағалау жоспарында өз жауапкершілігін, соның ішінде қауіпсіздікті қамтамасыз ету үшін жауапкершілігін түсінгендігіне көз жеткізу қажет. Сонымен қатар қызметкерлер туралы мәліметтерді тексеруге қатысты барлық ақпарат қолданыстағы заңнамаға сәйкес өңделуіне көз жеткізу керек (деректерді қорғау және т.с.с.).

6.4.1.3 Құпиялық туралы келісім

Қызметке қабылдау шарттарының бірі болып табылатын құпиялық туралы келісімге қызметкерлер қол қоюы қажет.

Аудит жүргізу жөніндегі басшылық:

Аудиторлар АҚБЖ қолдану саласына қатысты және қандай да бір құпия ресурстарға кіре алатын барлық қызметкерлер ұйыммен құпиялық туралы келісім бекіткеніне көз жеткізуі қажет. Келушілермен мұндай келісім жасау қажеттігі олардың қандай ақпаратты көре алуына және олар қандай іспен айналысуына байланысты (6.5.1.2-бөлімді қараңыз). Дәл осындай ережелер келісім-шарт бойынша қызмет етуші тұлғалар мен уақытша қызметкерлерге құпия ақпаратқа рұқсат берілген жағдайда қолданылады.

Кем дегенде кадрларды қамтамасыз етуші және ұйым арасындағы келісім-шартта бекітілген құпиялықты сақтау бойынша міндеттіліктердің болуын тексеріп, уақытша немесе келісім-шарт бойынша жалданатын қызметкерлер өздерінің міндеттіліктері туралы мәліметтенуіне көз жеткізу қажет. Жалпы алғанда, құпиялық туралы келісімдерді ұйымның кадр бөлімі жасауы қажет, сондықтан аталмыш бөлімде сәйкес формальды процедураның болын қадағалап, құжаттардың дер кезінде жүргізілетініне көз жеткізу қажет. Бұл орайда, жақын маңда қызметтен босатылған немесе босатылуға ниетті қызметкерлермен мұндай келісімдердің жасалуына ерекше назар аудару қажет.

6.4.1.4 Қызметке қабылдау шарттары

Қызметке қабылдау шартында қызметкердің қауіпсіздік ақпаратын қамтамасыз етуге жауапкершілігі анықталуы қажет.

Аудит жүргізу жөніндегі басшылық:

Аудиторлар қызметке қабылдау шарттарының қызметкердің қауіпсіздікті қамтамасыз етуге жауапкершілігін егжей-тегжей сипаттайтынына көз жеткізуі қажет. Қабылдау шартындағы сәйкес мәтін қолданыстағы заңнаманы орындауға байланысты міндеттермен қоса, нақты қызметпен байланысты, ұйымнан тыс немесе жұмыс уақытынан тыс жұмыспен, сондай-ақ келісім-шарт аясынан шығуы мүмкін міндеттерге байланысты барлық қауіпсіздік аспектілерін қамтуы қажет. Қызметке қабылдау шарты, сонымен қатар, қызметкердің ақпараттық қауіпсіздікті қамтамасыз ету бойынша өз міндеттерін орындамаған жағдайында әкелетін салдарын да сипаттауы қажет. Ұйымда қауіпсіздік аясында қызметкер міндетінің кез-келген өзгерісі жағдайында қызметке қабылдау шартын жаңарту жөніндегі шаралар жасақталуы қажет (мысалы, қызмет аясының кеңеюі немесе жаңа ақпараттық жүйелерді қолдану).

6.4.2 Пайдаланушыларды оқыту

Мақсаты: ақпараттық қауіпсіздікті бұзу қатері және олардың қалыпты жұмысы барысында ұйымда қабылданған ақпараттық қауіпсіздік саясатын қолдау қабілеті туралы пайдаланушыларға мәлімет беруді қамтамасыз ету.

6.4.2.1 Ақпараттық қауіпсіздік ережелеріне үйрету

Ұйымның барлық қызметкерлері, сондай-ақ қажет болған жағдайда, басқа ұйымдардың пайдаланушылары ұйымда қабылданған саясаттар мен процедуралар және олардың өзгерісі туралы қажетті мәліметтерді алуы қажет.

Аудит жүргізу жөніндегі басшылық:

Аталмыш басқару құралы жүйелік администраторлар, менеджерлер және қосымшалардың қатардағы пайдаланушылары, сондай-ақ жоғарғы басшылық пен кез-келген ақпаратты өңдеумен (мысалы, қағаз құжаттармен, телефон қоңырауларымен және т.б.) айналысатын тұлғалар сияқты ақпараттық жүйелердің пайдаланушыларымен қоса, барлық қызметкерлерге қолданылады. Баса назар аудару қажет бірінші мәселе - бұл оқыту шаралары алға қойылған мақсаттарға балама болып табылуына назар аудару; оқыту шаралары нақты қызмет талаптарына немесе оған байланысты қауіпсіздікті қамтамасыз ету жөніндегі міндеттер талаптарына сәйкес келуі қажет. Оқу қалай өткізілетін, оған ұйымның ішкі немесе сыртқы ресурстары қолданыла ма? Егер оқу ұйымның өз күштерімен жүргізілсе, ол қандай нұсқада өткізіледі: формальды оқу курсы ма әлде «жұмыс процессіндегі» стандартты оқу ма? Оқуды кім жүргізеді және оны жүргізуші тұлғалар қажетті біліктілікке ие ме? Егер оқу формальды емес түрде өткізілетін болса, онда

қарастырылатын тақырыптар аясы анықталған ба? Егер оқу ұйымнан тыс жүргізілетін болса, оқуды жүргізуші тұлға/ұйымдар кіммен құрылған? Оқу шаралары қандай құжаттарда белгіленген және бұл құжаттар оқу тақырыбы мен деңгейін айқындай ма?

Минимальды нұсқада ұйымның барлық қызметкерлері үшін қандай да бір формада кіріспе тренингі өткізілуі қажет. Ол қауіпсіздік саясаты мен жалпы қағидаларын, қолданылу саласын және т.б. мәселелерді қамтуы қажет. Мұндай тренинг қызметкерлердің есеп карточкаларында формальды түрде белгіленуі тиіс. Сонымен қатар, қауіпсіздіктің күрделі мәселелері үшін жауапты қызметкерлер үшін жеткілікті көлемде оқу шараларын өткізуді қамтамасыз ету қажет және онда келелі оқу материалдарының пайдалануын қадағалау қажет, ал оқу кестесі алдағы жұмыстарды ескере отырып құрылуы тиіс.

Қызметкерлер алдыңғы тәжірибеге немесе бұрын алған аттестациясына жүгініп, формальды оқуды алмастыруды өтінетін жағдайлар кездеседі (әсіресе, техникалық аспектілерге байланысты). Аудиторлар бұл жағдайға прагматикалық көзқараспен қарауы қажет және қызметкерлер білігі мен олардың сәйкес қызметтерін орындауды бағалау кезінде формальды оқу, біліктілік сынақтаулары нәтижесінде және тәжірибе негізінде алынған жалпы білімін назарға алғаны жөн. Егер қызметкер бұрынғы тәжірибесіне сүйенетін болса, бұрынғы білімдерінің ескірмегенін және релевантты еместігіне көз жеткізу қажет. Бұл тәжірибелер қандай ортада алынғанын және қызметкер білімінің қандай да бір тексерісі жүргізілгенін тексеру қажет. Көптеген ұйымдар қызметкердің резюмедегі өзі туралы жазған ақпаратының шынайылығына өте сенгіш келеді. Бірақ, тиісті білігі немесе тәжірибесі жоқ, маңызды қызметке алынған адам ұйымның өмірлік маңызы бар ресурстарына күрделі зиян тигізуі мүмкін, сондықтан бұл мәселеге баса назар аудару қажет. Аталмыш мәселе қызметке қабылданушыларды тексеруге де қатысты (жоғарыдағы 2.4.1.2. бөлімін қараңыз).

6.4.3 Қауіпсіздік жүйесіндегі оқиғалар мен оның бұзылуына шаралар қолдану

Мақсаты: қауіпсіздік жүйесіндегі оқиғалар мен оның бұзылуынан болған зияндарды азайту, сондай-ақ мұндай оқиғаларды зерттеп олардан сәйкес сабақ алу.

6.4.3.1 Қауіпсіздік жүйесіндегі оқиғалар туралы мәлімдемелер

Қауіпсіздік жүйесіндегі оқиғалар туралы дерек әкімшілік арналарына хабарлау қажет.

Аудит жүргізу жөніндегі басшылық:

Барлық ұйымдарда қауіпсіздік оқиғалары туралы хабар беруге арналған әкімшілік арналары мен сәйкес процедуралар қарастырылуы қажет. Аудиторлар мұндай процедуралардың оқиғалардың барлық мүмкін түрлерін

қамтитынын және балама жауапты шараларды қарастыратынын қадағалауы қажет. Егер ұйымда хабар беруді талап ететін оқиғалардың болмайтындығы жөнінде мәлімдесе және олар сәйкесінше хабар беру процессін көрсете алмаса, оқиғалар бәрібір орын алған, бірақ олар байқаусыз қалған деген ұйғарым жасауға болады. Осылайша оқиғалар жөнінде хабар беру процедуралары бұрын қауіпсіздік оқиғаларының болу-болмауына тәуелсіз әрбір ұйымның қол астында болуы қажет.

Сәйкес құжатта оқиғаның нақты анықтамасы толық сипатталған және жауапты қызметкерлер ұйымда қабылданған оқиға ұғымын жақсы түсінеді. Бірнеше мысалдарды қарастыру пайдалы болуы мүмкін: «Егер ұйым ғимаратындағы күзетілмейтін сейфтің ашылғанын байқасаңыз, қауіпсіздік оқиғасы болды деп санайсыз ба?»; «Егер қызметкер қателік бойынша бөтен біреудің жалақы ведомость алғанын хабарлаған болса, мұны қауіпсіздік инциденті деп атауға бола ма?» және т.б. Мұндай мысалдар нақты жағдайға қолданылатыны анық, алайда қызметкерлердің жауабы көрнекі және мұндай мәселелерге олардың жалпы ұстанымын көрсетуі мүмкін. Егер ұйым оқиғалар туралы есебін ұсынған болса, аталмыш оқиғаға қандай әрекет жасалуын сараптаңыз: ол жағдай реттелді ме, оның болуына себепші болған жағдайлар зерттелді ме және зерттеулер нәтижесі оқиғаның болуы туралы хабарлаған қызметкерлерге ұсынылды ма (әрине, бұл ақпарат құпия болып табылмаса).

6.4.3.2 Қауіпсіздік жүйесіндегі әлсіз тұстар туралы мәлімдемелер

Ақпараттық сервистердің пайдаланушылары сервистер немесе жүйелердегі байқалған немесе болжанған кез-келген әлсіз тұстарын немесе жүйелер мен сервистерге кез-келген қатерлерді тіркеуге және оларды хабарлауға міндетті.

Аудит жүргізу жөніндегі басшылық:

Қорғаныстағы болжамды немесе шынайы әлсіз тұстарын хабарлау үшін қауіпсіздік оқиғаларында қолданатындарға ұқсас мәлімдеу процедуралары қарастырылуы қажет. Барлық қызметкерлер қауіпсіздікті қорғау жүйесіндегі әлсіз тұстар туралы хабарлау қажеттігін ұғынуы қажет. Бұл тек ақпаратты өңдеу саласына ғана қатысты емес - ғимараттағы ашық терезе дәл сондай қорғаныстағы әлсіз тұс болуы мүмкін. Мәлімдеу процедуралары қызметкерлерге анықталған әлсіз тұстарды, мысалы, рұқсатсыз қолжетімділікті алу сияқты әлсіз тұстарды пайдалануға тиым салушы нұсқамаларды қамтуы қажет. Тіпті олардың мақсаты қорғаныстағы әлсіз тұсты растау болып табылса да, мұндай әрекеттер күрделі зиян тигізуі мүмкін.

6.4.3.3 Бағдарламалық құралдар дағы кемшіліктер туралы мәлімдеме

Бағдарламалық құралдар дағы кемшіліктер туралы мәлімдеу процедуралары жасақталуы қажет.

Аудит жүргізу жөніндегі басшылық:

Аталмыш проблемалар жоғарыда сипатталған қорғаныстағы тікелей әлсіз тұстар және қауіпсіздік оқиғаларымен жұмыс жөніндегі процедураларға сай келуі мүмкін, алайда, мәлімдеме нысаны пайдаланушыдан кемшіліктің нақты белгілері мен компьютермен берілген кез-келген хабарларды талап ететініне көз жеткізу қажет - бұл деректер БҚ кемшілігінің себебін зерттеуге көмектеседі. Мәлімдеу процедуралары (қауіпсіздік оқиғалары мен қорғаныстағы әлсіз тұстар жағдайы сияқты) кез-келген кемшіліктерді жауапты тұлғаларға мәлімдеуді қамтамасыз етуі қажет, себебі кейбір пайдаланушылар ұсақ келеңсіздіктер деп қабылдайтын жағдайлар уәкілетті мамандармен сараптау кезінде қауіпсіздіктің маңызды проблемасы ретінде танылуы мүмкін.

Дер кезінде мәлімдеу өте маңызды; мысалы, вируспен залалдану мүмкіндігі туралы ертерек хабарлау үлкен зияндардың алдын алуға мүмкіндік береді. Аудиторлар коррекциялық шараларды мұқият сараптауы қажет (кезде сәйкес БҚ түзетуге болады, ал кейбір жағдайларда жаңа нұсқасының шығуын күту және тығырықтан шығудың басқа жолдарын қарастыру қажет): қабылданған шаралар қаншалықты тиімді, басқа қандай да бір процедураларды өзгерту қажет пе, аталмыш жағдай туралы ақпарат қызығушылық танытушы тұлғалар арасында қалай таратылады. Қажет етілген өзгертулер бекітілді ме? Егер жағдай бөгде тараптардың тұлғаларын/мекемелерін тартуды талап етсе (мысалы бағдарламаны жеткізуші), ақпарат қандай жолмен ұсынылады және ақпаратты тарату кезінде ұйым қауіпсіздігі үшін жекелеген проблема туындамай ма?

Қауіпсіздік оқиғалары, қорғаныстағы әлсіз тұстармен бағдарламалық құралдар дағы кемшіліктер туралы мәлімдемелер мен есептер сәйкес байланыс тұлғасына немесе тұлғаларға жіберіледі. Таңдалған байланыс көздері ең тиімді, қажетті жағдайда қолжетімді және сәйкес білімдерге ие екенін тексеру қажет. Проблема күрделілігі талап еткендей мәлімдемелер жеткілікті түрде мұқият қарастырыла ма, жоғары басымдылық беру процедуралары қарастырылған ба, проблема туралы хабарлаған тұлғалармен кері байланыс орнатылған ба?

6.4.3.4 Болған оқиғадан сабақ алу

Орын алған оқиғалар мен кемшіліктердің сандық бағасы мен типтерінің мониторингі, ауқымы мен құнын анықтау үшін тетіктер жүзеге асырылуы қажет.

Аудит жүргізу жөніндегі басшылық:

Аудиторлар ұйымдар бұрын болған жүйе мен бағдарламалық құралдар дағы кемшіліктер мен қауіпсіздік оқиғаларына әрекет етудің барлық мысалдарын сараптауы қажет. Оқиғалардың сандық бағасы мен ауқымын анықтау қалай жүргізілетіні, сондай-ақ оқиғалармен жұмыс процедуралары

бұрынырақ болған оқиғаларға және болашақта болуы мүмкін оқиғалар типіне қаншалықты сәйкес келетінін анықтау қажет.

Егер ұйым сабақ алу үшін оқиғалар жеткіліксіз болды немесе релевантты ақпарат жоқ деп мәлімдейтін болса, мұндай мәлімдемелерге мұқият қарау қажет, себебі олар оқиға туралы мәлімдеу процедураларының қолданбауы немесе ондай процедуралардың болмауын білдіреді. Мұндай жағдайда, аудитор жағдайлардың қосымша анализін жүргізуі қажет және оны ұйымдағы тиісті тұлғалармен бірлесіп талқылауы қажет.

Ұйымда жүйе мен бағдарламалық құралдардағы кемшіліктер мен қауіпсіздік оқиғаларына әрекет ету процедуралары мен жоспарлары қарастырылуы қажет. Оларға проблемалардың қайта туындауын болдырмауға, шығындарды шектеуге, қажетті куәліктердің жиналуын қамтамасыз етуге және келешекте одан да жедел және тиімді әрекет етуге мүмкіндік беретін процедуралары мен басқарудың қосымша құралдарын жүзеге асыру кіруі қажет. Болған оқиғалардан сабақ алу, сонымен қатар, оларды тренингтер және қауіпсіздік жөніндегі таныстыру бағдарламалар аясында шынайы мысалдар ретінде қолданылады.

6.4.3.5 Тәртіптік процедура

Қызметкерлердің ұйымда қабылданған қауіпсіздік процедуралары мен саясатты бұзуы формальды тәртіптік процедура аясында қарастырылуы қажет.

Аудит жүргізу жөніндегі басшылық:

Ұйым үшін бұл мәселе сындарлы болуы мүмкін, бірақ қауіпсіздіктің бұзылуына адекватты әрекет ету үшін сәйкес процедурасының қай та қарастырылуы өте маңызды болып табылады. Тәртіптік процедураның детальдері, сондай-ақ барлық қатысушы тұлғалар үшін әділ қараудың кепілі қызметкерлердің барлығына хабарлануы қажет. Егер тәртіптік процедура жөнсіз жүзеге асырылған болса, қызметкерлерді орынсыз қызметтен босату немесе басқаша құқықтарын бұзуға байланысты арыз-талаптар беру мүмкіндігі болады. Кез-келген жағдайда нақты анықталған тәртіптік процедура басқару тиімділігі онсыз төмендеуі мүмкін маңызды фактор болып табылады. Аудиторлар тіркелген қауіпсіздік оқиғаларын талдап, тәртіптік жазалауды қолдану критерийлерін қарастыруы және аталмыш процедуралар тиімді қолданылатынына көз жеткізуі қажет.

6.5 Физикалық қауіпсіздік және қызмет ету ортасының қауіпсіздігі

6.5.1 Қорғалған салалар

Мақсаты: Өндірістік орындарға және ақпараттық серверларға заңсыз физикалық кіруді, оларды зақымдауды және олардың қызметіне килігуді болдырмау.

6.5.1.1 Қауіпсіздіктің физикалық периметрлері

Ұйымдар ақпаратты өңдеу құралдары орналастырылатын салаларды қорғау үшін қауіпсіздік периметрлерін пайдалануы қажет.

Аудит жүргізу жөніндегі басшылық:

Барлық ұйымдар өз ресурстарының физикалық қорғаныс құралдары мен тәсілдерін көрсетуі қажет. Егер ірі объектілер туралы сөз қозғалатын болса, қауіпсіздік процедуралары қандай қорғаныс шаралары қолданылатыны, олардың қалай бақыланатыны және ол объектіге кім кіре алатыны жөнінде толық сипаттама беруі қажет. Ұйымда жүзеге асырылған физикалық қорғанысқа баға беру үшін аудиторлар мүмкін кіру жолдарын талдауы қажет: ашық өрт жолдары/сатылар, келушілерді қабылдауға арналған бақыланбайтын бөлмелер, бөтен кіруге рұқсат қағаздарын және кілттенбеген шкафтарды пайдалану – мұның бәрі де қауіпсіздікке тікелей қатер төндіреді және тиісті түрде бекітілуі қажет.

Физикалық қорғанысты жүзеге асырудың бір бөлігі физикалық периметрлерді қолдану болып табылады, сондықтан ұйым өзінің физикалық периметрлері мен олар жүзеге асыратын қорғаныс туралы мәліметтерді беруі қажет (бұл ақпарат қатерлерге баға беру жөніндегі деректерге тігілуі қажет).аудиторлар сонымен бірге ғимаратқа қалай кіруге болады және ол қалай бақыланады, ұйым қайда орналасқан, және қолданылатын басқару құралдары оның мұқтаждығын қалай өтейді, сондай-ақ қорғаныс құралдарын өтіп кетуге бола ма деген мәселелерді анықтауы қажет.

6.5.1.2 Ғимаратқа кіруді бақылау

Қорғалған салалар оларға тек сәйкес уәкілеттік алған қызметкерлер ғана кіре алуы үшін, ғимаратқа кіруді қадағалау үшін қажетті құралдармен қорғалған болуы қажет.

Аудит жүргізу жөніндегі басшылық:

Аудиторлар ғимаратқа кіруді бақылаудың жүзеге асырылуын тексеріп, сәйкес рұқсаты жоқ барлық тұлғалардың ғимаратқа кіруін шектеу үшін осы шаралардың жеткілікті екеніне көз жеткізуі қажет. Қызметкерлер идентификациялық төсбелгілерін таға ма және оларды тағу міндетті шарт болып табыла ма? Мұндай төстаңбалар келушілерге беріле ме, олардың келіп/кетуі тіркеле ме, олардың ұйым ішінде жүруіне қандай шектеулер қойылады? Төстаңбалары жоқ тұлғалар тексеру үшін тоқтатыла ма? Соңғы жайтты аудиторлар келуші болып табылатындықтан өз тәжірибесінде тексере алады.

Аудиторлар сонымен қатар кіру бойынша бұрынғы тіркеу жазбаларын тексеруі және аталмыш ұйымда ғимаратқа кіру құқығын жаңарту және тексеру процедуралары қарастырылғанын қадағалауы қажет. Кіруге рұқсат немесе тиым салу әр түрлі формада айқындалуы мүмкін: олар лауазымдық нұсқамаларға енгізілуі мүмкін, процедуралар сипатында болуы мүмкін

немесе шектеулер күшіне енетін жерде тікелей белгіленуі мүмкін (мысалы, кіру құқығы шектелген бөлме есігіндегі тақтайша). Аудиторлар мұндай тәсілдердің әрбірінің қолданысын бағалауы қажет.

6.5.1.3 Кеңселерді, бөлмелер мен жабдықтарды қорғау

Олардың қауіпсіздігіне ерекше талаптар қойылатын кеңселер, бөлмелер мен жабдықтарды қорғау үшін арнайы қорғалған салалар құрылуы қажет.

Аудит жүргізу жөніндегі басшылық:

Қорғалатын салаға қамтамасыз етілетін қорғаныс деңгейі құпия ақпаратпен жұмыс істеу процедураларына сәйкес, онда сақталатын ақпарат құпиялылығының максималды деңгейіне сәйкес болуы қажет. Бұл мәселе тәуекелдерді бағалауға тікелей байланысты, және аудиторлар осыны назарға ала отырып, ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі шаралар сәйкестендірілген, ал қорғаныстың жүзеге асырылған құралдары оларға сәйкес келетініне көз жеткізуі қажет.

Қолжетімділікті басқарудан басқа, аудиторлар электр энергиясының берілуі, төтенше жағдайларда қорғау, табиғи апаттардан қорғау (өрт қауіпі бар ма, бөлменің су астында қалуы мүмкін бе) сияқты қауіпсіздік және қолжетімділікті басқа да аспектілерін зерттеуі қажет және мұндай қауіптер төнген жағдайда оларды қалай алдын алу немесе олардың салдарын қалай төмендету қарастырылғанын анықтауы керек. Сонымен қоса, төмендегі «Жабдықтарды орналастыру және қорғау» және «Электр қорек көздері» (6.5.2-т) бөлімдерін қараңыз.

6.5.1.4 Қорғалған салаларда жұмыс жасау

Қорғалған салаларда қауіпсіздікті арттыру мақсатында бақылаудың қосымша құралдары және қорғалған салаларда жұмыс жасау ережелері қолдануы қажет.

Аудит жүргізу жөніндегі басшылық:

Қорғалған салаларда жұмыс жасаушы қызметкерлер үшін ұйымда жұмыс жасалатын құпия және сындарлы ақпарат үшін жеткілікті болып табылатын қауіпсіздік деңгейін қамтамасыз етуші ерекше басқару құралдары қолданылуы қажет. Аудиторлар келесі жағдайларды тексеруі тиіс:

– қорғалған салаларға тек арнайы рұқсаты бар тұлғалардың ғана кіруіне мүмкіндік беруші жеке қолжетімділікті басқару құралдарының болуы;

– компания қызметкерлеріне қорғалған салаларда жүргізілетін жұмыстар туралы қаншалықты мәлім екенін және бұл мәліметтердің қажетті шектен аспауын тексеру;

– ақпаратты қорғалған аймаққа енгізу және одан шығару қаншалықты оңай (ақпарат қағаз құжаттарда болуы немесе дискте жазылуы мүмкін);

– қорғалған аймаққа суретке түсіру, бейне-, аудио- немесе басқа д ажазу құралын енгізу, сондай-ақ оны қолды немесе автоматты режимде жазу үшін қолдану мүмкін бе;

– мұндай аймақтарда жұмыстарды бақылау жеткілікті түрде жүзеге асырыла ма және қажет етілген жағдайда екі еселеген бақылау механизмдері қарастырылған ба.

6.5.1.5 Оқшауланған қабылдау және түсіру орындары

Қабылдау және түсіру орындары бақылануы қажет және мүмкіндік болса, рұқсатсыз енудің алдын алу мақсатында ақпаратты өңдеу құралдарынан оқшауланууы қажет.

Аудит жүргізу жөніндегі басшылық:

Аталмыш басқару құралы қабылдау және түсіру операциялары кезінде қауіпсіздік оқиғаларын болдырмауға арналған. Жүктерді түсіру бөгде қызметкерлерімен жүргізілуі мүмкін, олардың ұйым аймағында жүруін шектеу қажет. Егер жеткізілген жүктерді қабылдау кезінде бастапқы тексеріс жүргізілмеген және тесттеуден өткізілмеген болса немесе сақтау шарттары орындалмаған болса, жеткізілген жүктер қауіп төндіруі мүмкін. Ұйым территориясынан шығарылатын жүктер ішіне абайсызда құпия ақпарат түсуі мүмкін. Нақты жағдайда қолданылатын барлық қатер салалары тәуекелдерді бағалау негізінде анықталуы тиіс, ал ұйым тікелей қауіпсіздікті бұзудың алдын алу және олардың салдарын төмендету үшін адекватты шараларды қолдануы қажет. Мысалы, жеткізілген жүктерді кім қабылдайды: оның сұранысы бойынша жеткізілген қызметкермен, қойма қызметкерімен немесе қабылдау бөлмесінің хатшысымен? Жеткізілген жүктер ары қарай қайда бағытталады: олар бірден қорғалған аймаққа жеткізіледі, қоймаға жөнелтеді немесе адресаттың өзіне тікелей жіберіледі?

6.5.2 Жабдықтарды қорғау

Мақсаты: Ресурстардың жоғалуын, зақымдалуын немесе ашылуын, сондай-ақ ұйым жұмысындағы іркілістің алдын алу.

6.5.2.1 Жабдықтарды орналастыру және қорғау

Жабдықтар сыртқы ортаның әсеріне байланысты қатерді және рұқсатсыз кіру мүмкіндігін азайтатындай етіп орналастырылған немесе қорғалған болуы қажет.

Аудит жүргізу жөніндегі басшылық:

Ұйымдар қолданатын жабдықтардың қалай қорғалғанын көрсетуі қажет. Жабдықтар сигнализацияның іске қосылуын болдырмай бөлме ішіне оңай енуге болатын терезе сияқты, тікелей қатер аймақтарынан алыста орналастырылуы қажет. Сонымен қатар, компьютерлік терминалдардың экрандары қорғалған аймақтардан тысқары жерден қарастырыла алатынын ескеру қажет.

Бірқатар жағдайларда компьютерлік жабдықтарды қызметкерлердің жұмыс үстеліне орнату қажет. Қасақана зақымдаудан қорғаумен қатар, жабдықтарды бөлмедегі жөнсіздік, қадағаланбайтын кіріс, тұрақсыз жиһаз, төгілген сұйықтық және т.б. кездейсоқ зақымдаудан, сондай-ақ қоршаған ортаның жағымсыз әсерінен; су, химикаттар, өрттен қорғау қажет. Ұйымда сәйкес қорғаныс шаралары жасақталғанын және жүзеге асырылғанын тексеріңіз.

Тексеру компьютерлік техника орналасқан бір жермен ғана шектелмеуі керек. Көршілес бөлмелерде өрт немесе су басу қатерлерінің болуын тексеріңіз. Ірі ұйымдарда әдетте, ғимарат (кеңсе) жоспары бар болады. Онымен танысып, қауіпсіздік тұрғысынан жабдықтардың орналасуының адекваттығына баға беріңіз.

6.5.2.2 Электр қорегінің көздері

Жабдықтар электр қорегі жүйесіндегі үзілістер мен электр желісіндегі басқа да ақаулардан қорғалған болуы қажет.

Аудит жүргізу жөніндегі басшылық:

Электр энергиясын берудегі кідірістен қорғаудың қажетті деңгейі сақталатын ақпараттың сындарлы және қауіпсіздік талаптарына, сонымен қатар жүйе құрамындағы жабдықтарға байланысты (мысалы, жүйе қолжетімділігі бойынша талаптар жоғары болса, электр қорегін қамтамасыз етуге арналған басқару құралдары да күрделірек болуы қажет). Кез-келген жағдайда, аудитор тым болмаса қорғаныстың минимальды деңгейі – кернеу өзгерісін біркелкі ету жүзеге асырылғанына көз жеткізуі қажет.

Одан да күрделірек талаптар қойылған жағдайда, жеткілікті резервтік көздердің және резервтік көшіру жүйелерінің болуын тексеріңіз: қосымша генераторлар, ҮҚК, дискілік RAID-массивтер және т.б. Егер мұндай жабдықтар бар болса, келесі жағдайларға назар аударыңыздар: резервтік схема бойынша электр энергиясы жеткілікті өндіріле ме; резервтік көздер қандай уақыт аралығында жұмыс істейді; бұл уақыт аралығы ұйымның келісім-шарттық міндеттеріне сәйкес келе ме; резервтік қоректендіру жүйелерін тестілеу және оған қызмет көрсету кезінде өндіруші ұсыныстары сақтала ма. Аудитор сонымен қоса, электр энергиясы тоқтаған жағдайда ұйым бөлмелері апаттық жарық беру жүйелерімен қамтамасыз етілгенін тексеруі қажет.

6.5.2.3 Кабельдік желістің қорғалуы

Электр қорегінің кабельдері мен деректерді өткізу немесе ақпараттық сервистерді қолдау үшін қолданылатын желілік кабельдер ақпаратты кесіп алу немесе зақымдау мүмкіндігінен қорғалуы қажет.

Аудит жүргізу жөніндегі басшылық:

Кабельдік қосылыстар мен ағытпалардың жалпы күйіне баға беру қажет: олар дұрыс жалғанған немесе жүргізілген бе, кабельді дұрыс орнатпағандықтан және т.б. себептерден туындаған қауіп жоқ па.

Коммуналдық қосылыстардың ажыратпасы пайдаланушылардың бір бөлігі үшін сындарлы мәселе болуы мүмкін. Аудиторлар қандай қатерлердің коммуникация мәселелеріне байланысты екенін анықтап, қорғаныстың тікелей әлсіз тұстарын айқындауы қажет: ғимараттар мен бөлімдер арасында салынған желілік кабельдер, болуы мүмкін зақымдалудан немесе рұқсатсыз тыңдалудан қорғалмаған телефон желістері.

6.5.2.4 Жабдықтарға техникалық қызмет көрсету

Жабдықтың тұрақты қолжетімділігі мен бүтіндігін қамтамасыз ету мақсатында оған тиісті техникалық қызмет көрсетілуі қажет.

Аудит жүргізу жөніндегі басшылық:

Аудиторлар ұйымда жеткізушімен кеңесілген және ұсынылған спецификацияларға сәйкес кезеңділікпен жабдықтардың күтімін қамтамасыз етуге мүмкіндік беретін басқару құралдары жүзеге асырылғанына көз жеткізу қажет. Сонымен қатар, ауа сүзгіштерін, принтер және магнитті таспалардағы жинағыштардың механикалық бөлшектерін тазарту сияқты, қарапайым шараларды жүргізу күрделі істен шығу жайттарының алдын алуға көмектесуі мүмкін. Компьютерлерінің тұрғылықты дисктерін тұрақты дефрагментациялау сияқты қатардағы операциялар жұмыс тиімділігіне едәуір әсер етуі мүмкін.

Ұйымда қызмет көрсету бойынша шаралардың қандай процедуралары қарастырылғанын анықтаңыз, олардың жеткілікті болуын тексеріңіз және олардың белгіленген процедураларымен сәйкестігін анықтау үшін қызмет көрсету бойынша жазбаларды тексеріңіз. Ұйымда жұмыстың кідірістері туралы хабарлауға арналған формальды тетігі қарастырылуы қажет. Ондайдың болуын қадағалаңыз, сонымен қатар анықталған кемшіліктер және оларды жою туралы жазбаларды тексеріңіз. Жабдықтарға сервистік қызмет көрсету бойынша шаралар тек сәйкес рұқсаты бар қызметкерлермен жүргізілетініне, ал қызмет көрсету жөніндегі процедуралар бөгде тұлғалармен жүргізілген жағдайда, оларды жауапты қызметкерлер сүйемелдейтініне көз жеткізу қажет.

6.5.2.5 Ұйымнан тысқары қолданылатын жабдықтарды қорғау

Ұйым аумағынан тыс ақпараттарды өңдеуге арналған жабдықтардың кез-келген қолданысы басшылықпен рұқсат етілген болуы қажет.

Аудит жүргізу жөніндегі басшылық:

Аталмыш басқару құралы ұйым аймағынан тысқары қолданылатын кез-келген жабдық қауіпсіздігін қамтамасыз етеді. Негізгі қызметінің түріне байланысты ұйымның бір бөлігі үшін бұл проблема көкейтесті болып

табылмайды, бірақ көптеген мекеме үшін бұл мәселе жеткілікті түрде маңызды.

Ұйымдағы қорғалған ортадан тысқары жабдықтарды пайдалану қауіпсіздік саласындағы бірқатар проблемалармен және қосымша қатерлерге байланысты. Сондықтан аудиторлар негізгі аумақтан тысқары физикалық қауіпсіздікті қамтамасыз етуге бағытталған басқару құралдары ұйымдағы қауіпсіздіктің стандартты деңгейіне сәйкес қорғаныстың жеткілікті деңгейін қамтамасыз ететіндігіне көз жеткізуі қажет. Негізгі аумақтан тыс қолданылатын жабдықтардың бақылаусыз қалмайтынын, ал қажет жағдайларда балама сақтандыру қамтамасыз етілетінін кепілдеуші процедуралар мен ұсыныстар қарастырылуы қажет.

6.5.2.6 Жабдықтарды сенімді түрде кәдеге жарату немесе оны қайта пайдалану

Жабдықты кәдеге жарату немесе қайта пайдаланудан бұрын ондағы ақпаратты өшіру қажет.

Аудит жүргізу жөніндегі басшылық:

Ұйымда кәдеге жаратуға арналған жабдықтар мен қандай да бір жолмен қадағаланбайтын басқа да жабдықтардан деректерді өшірудің тиімді процессі қарастырылуы қажет. Аудиторлар пайдаланушылардың аталмыш жағдайда қауіпті жете түсінетіндігін, ал ұйымда кәдеге жаратуға арналған құрылғыларда құпия ақпараттың болмайтындығын кепілдейтін тиімді құралдарының болуына көз жеткізуі қажет. Магнитті таратушылардан ақпаратты өшіру қауіпсіз тәжірибе болып табылмайды: бірқатар жағдайларда деректер өшірілген соң да оқылады. Деректер толық өшірілуі үшін ақпаратты бірнеше рет форматтау немесе қайта жазу қажет болуы мүмкін. Сәйкес саясат ақпарат таратушылардың барлық түріне таратылуы мүмкін – мысалы, құпия ақпараты бар таратушылардың сәйкестендірілуін барынша күрделендіру үшін барлық жазба/жапсырмаларды жою қажет болуы мүмкін.

Қатерлердің сипатына байланысты ең тиімді әдіс дисктер мен магнитті таспаларды физикалық жою болуы мүмкін; бұл сонымен қатар компьютерлерге орнатылған тұрғылықты дисктерге де қатысты болуы мүмкін. Кейбір ұйымдар мұндай әдісті шамадан тыс қатаң деп санауы мүмкін, бірақ ақпараттың магнитті таратушылары онша қымбат емес және оларды жоюды шығыны құпия және әшкерелейтін деректерді жоғалтудан гөрі арзанырақ болатыны сөзсіз. Сонымен қатар, сервиске жөндеу үшін берілетін жабдықтарға назар аудару қажет: маңызды ақпаратты түрлендіру немесе ашу мүмкіндігі тексеріле ме?

6.5.3 Басқарудың жалпы құралдары

Мақсаты: ақпараттың және ақпараттық жүйелер жабдығының ұрлануын немесе әшкереленуін болдырмау.

6.5.3.1 Компьютерлік терминалдар және жұмыс үстелін пайдалану саясаты

Ұйымдар ақпараттардың рұқсатсыз ашылуы, жоғалуы және зақымдалуының қатерін азайтуға бағытталған компьютерлік терминалдар мен жұмыс үстелін пайдалану ережелерін бекітуі қажет.

Аудит жүргізу жөніндегі басшылық:

Аталмыш басқару құралының мақсаты кез-келген текті құпия ақпарат (электронды, қағаз формадағы, таратушыға жазылған және т.б.) тиісті бақылаусыз қалдырылмайтынын кепілдеу, сондай-ақ ақпараттың жоғалуынан (әшкерелеуден, түрлендіруден және ашылудан) қорғанысты қамтамасыз ету болып табылады. Қарастырылған шаралар жұмыс уақытында, сондай-ақ жұмыс уақытынан тыс кездері қолданылуы қажет. Сонымен қатар, «Ақпаратты жүйелеп топтастыру» бөлімінде сипатталған қағидаларға сәйкес ақпаратты тиісті түрде жүйелеп топтастыру қажет.

Сыртқы қызметкерлер тарапынан (мысалы, сыпырушы) құпия ақпаратты ашу қауіпін ескеруші қорғаныс шараларын қолға алу қажет. Сонымен қатар, жұмыс күні аралығында үстелдер, қағаз қоюға арналған шкафтар, сейфтер және т.б. қараусыз қалдырылған кезде не болатынын тексеру қажет: ол қауіпсіздікті бұзуға әкелмей ме? Сонымен қатар, қызметкерлер болмауының ұзақтығына тәуелсіз, қызметкерлер болмағанда компьютерге кіру мүмкіндігі бар екенін есте сақтау қажет. Мұндай жағдайда парольмен қорғалған экранды қорғағыштарды пайдалану, компьютерді сөндіру немесе компьютерлік терминалдарды пайдалану саясатымен қарастырылған басқа кез-келген басқару құралдарын пайдалану қажет.

Бірқатар жағдайларда «Басқару құралдары» бөлімінде сипатталған логикалық қолжетімділікті басқарудың қосымша құралдарын пайдалану қажет. Егер барлық аймақ үшін қауіпсіздіктің ортақ сәйкес деңгейі қамтамасыз етілген болса, ал оның аясындағы қызметкерлер кіру кезінде тексеруден өтсе, қосымша шараларды қолдану міндетті емес. Жалпы алғанда қауіпсіздік саясаты нақты айқындалғанын, ал қызметкерлер сәйкес процедуралар туралы мәліметтенгенін және оларды орындайтындығын тексеріңіз.

6.5.3.2 Мүліктерді ұйымнан тыс шығару

Ұйымға тиесілі жабдықтарды, ақпаратты немесе бағдарламалық құралдарды ұйымнан тысқары шығаруға басшылық рұқсаты берілуі қажет.

Аудит жүргізу жөніндегі басшылық:

Көптеген ұйымдар қызметінің спецификасы тұрақты түрде қызметкерлердің жабдықтарды, деректерді және құжаттамаларды территориядан тыс шығаруын талап етуі мүмкін.

Бұл үйде жұмыс істеу кезінде, кездесулер және мәжілістер өткізу және т.б. жағдайларда талап етілуі мүмкін. Бірқатар ұйымдар үшін мұндай

жағдайларды қадағалау күрделі мәселе болуы мүмкін. Аудитор ең алдымен ұйымда бұл мәселенің өзін, сондай-ақ оның шешімін басқарудың тиімді құралдарын сәйкестендіргеніне көз жеткізу қажет. Бірнеше мүмкін нұсқалар бар:

– Кез-келген құпия ақпаратты шығаруға тиым салынған. Бір қарағанда бұл ең қарапайым шешім, бірақ көптеген ұйымдар үшін мұндай ұстанымды қолдану қиынға соғуы мүмкін. Мұндай шешім қауіпсіздік талаптары өте қиын ұйымдар үшін сәйкес келеді.

– Құпия ақпаратты шығаруға таңдалған басқару құралдарына сәйкес жол беріледі. Мұнда ұйымнан қажетті басқару құралдарының қатаң тізімдемесі мен ақпаратты шығаруға рауалы нақты анықтама қажет.

– Құпия ақпаратты шығару ешқандай жолмен қадағаланбайды. Бұл нұсқа үлкен қауіп төндіруі мүмкін және оны жүзеге асыру ұйымнан тысқары құпия ақпаратпен жұмысты реттеуші қосымша басқару құралдары болмаған жағдайда ұсынылады.

Аудитор ұйым саясатында қандай ұстаным таңдалғанын анықтағаны жөн, содан соң сәйкесінше құжатталған процедуралармен танысуы қажет. Мүлікті енгізу/шығару кезінде тіркеу жүйесі қолданыла ма, қандай рұқсаттар талап етіледі және олар қайда белгіленеді, бұл ережелер барлық заттар үшін қолданыла ма, әлде шектеулі түрлеріне ғана қатысты ма? Басшылық тарапынан нормалардың орындалуы қалай қадағаланады? Шамадан тыс қатаң тәртіп қабылданған процедураларды айналып өтуіне әкелуі мүмкін, ал тым жұмсақ тәртіп қауіпсіздіктің өрескел бұзылуына әкеледі. Құпиялықты сақтау туралы келісім ұйым территориясынан тыс қызметкердің иелігіндегі ақпарат үшін жауапкершілікті қарастыра ма? Көптеген қызметкерлер ықшам компьютерлерді пайдаланады: ұйымда олармен және онда қамтылған құпия ақпараттармен жұмыс істеуге арналған қандай басқару құралдары жүзеге асырылған? Компьютер жадына немесе электронды таратушыға жазылған ақпарат жасырыла алады (мысалы файл атауын өзгерту); осымен күрес үшін іздеу құралдары қажет етіле ме, егер иә болса, оларды қашан қолдану қажет?

Қазіргі кезде коммуникация құралдарының қолжетімділігі ақпаратты ұйымнан тыс шығару үшін физикалық таратушыларды қолдану міндетті болмайтынын білдіреді; аудиторлар мысалы, Интернет арқылы кіру кезінде деректерді өткізудің қандай бақылау механизмдері қолданылатынын анықтауы қажет.

6.6 Компьютерлік жүйелеріне және есептеу желілеріне әкімшілік ету

6.6.1 Операциялық процедуралар мен міндеттер

Мақсаты: Ақпаратты өңдеу үшін қолданылатын құралдардың дұрыс және сенімді қызмет етуін қамтамасыз ету.

6.6.1.1 Құжатталған операциялық процедуралар

Қауіпсіздік саясатында сәйкестендірілген операциялық процедуралар құжатталып, бекітілуі қажет.

Аудит жүргізу жөніндегі басшылық:

Аудиторлар құжаттамада шынайы айқындалу және ұйымның қажет болған салаларында реттілікпен пайдалану нысанына ұйымның операциялық процедураларын зерттеп, талдауы қажет. Аталмыш процедуралардың толықтығын тексеру үшін аудиторлардың ұйым жұмысы мен әр түрлі операциялық процесстер туралы жалпы түсінігі болуы қажет.

Қосымша, осы процедуралардың пайдаланылуын, қолдануын және орындалуын тексеру қажет. Сонымен қатар, сәйкес рұқсатсыз процедураға өзгерістер енгізуді мүмкінсіздігін, сондай-ақ оларды және олармен байланысты кез-келген басқару құралдарын айналып өту мүмкінсіздігін кепілдеуші тексерісті жүргізу қажет.

Желілік сервистерді пайдалану және әкімшілік ету жауапкершілігі жекелеген бөлімшелерге немесе тіпті жекелеген ұйымдарға артылған. Сәйкесінше аудитор бұл мәселенің ұйымда қандай жолмен шешілгенін түсінуі қажет және сервистік шаралар мен процедуралар сәйкес деңгейде дұрыс құжатталғанына көз жеткізуі қажет. Кейбір салаларда жұмыстарды жүргізу жөніндегі нақты нұсқамалар қажет. Сонымен қатар, пайдалану және әкімшілік ету процессінде жабдықтарды жеткізушілердің құжаттамасы белсенді түрде қолданылатыны айқын, сондықтан оның болуын және мерзімділігін тексеру қажет.

6.6.1.2 Өзгерістерді бақылау

Ақпаратты өңдеу жүйелеріндегі және құралдарындағы барлық өзгерістер қадағалануы қажет.

Аудит жүргізу жөніндегі басшылық:

Аудитор ақпараттарды өңдеуде қолданылатын құралдардағы өзгерістерді бақылау бойынша жауапты тұлғалар мен формальды процедуралардың болуын тексеруі қажет. Мұндай өзгерістердің барлығы қадағаланып, ал нақты өзгерістердің мән-жайы сәйкес хаттамаларда тіркелуі қажет. Бірде-бір өзгеріс оның енгізілуінен болуы мүмкін зияндарды бағалаусыз жүргізіле алмайтыны кепілденуі қажет, ал әрбір ұсынылған өзгерту сәйкес түрде бекітілуі қажет.

Ұйымда проблемалық жағдайларда әрекет ету тәртібін сипаттаушы процедуралар қарастырылуы қажет; сондай-ақ өзгертулерді енгізу жөніндегі жұмыстар қажет болған жағдайда бастапқы қалпына келуге мүмкіндік беруші сәйкесінше қайтару процедуралары болған жағдайда ғана басталатынын кепілдеу қажет. Аудиторлар бұл процедуралардың енгізілген өзгертулер туралы барлық мүдделі қызметкерлерге хабарлау жүйесін қамтитынына көз жеткізуі қажет. Егер операциялық өзгертулер

қосымшалардағы өзгерістерге әкелетін болса, мұндай өзгертулерді де интеграциялау қажет.

6.6.1.3 Жағдайларға әрекет ету процедуралары

Қауіпсіздік жүйесіндегі оқиғаларға дер кезінде, тиімді және ұйымдасқан түрде әрекет ету үшін және оқиғаларға байланысты деректерді жинақтау үшін (бақылау журналдары сияқты), сәйкес процедуралар мен әкімшілік міндеттер анықталуы қажет.

Аудит жүргізу жөніндегі басшылық:

Аудитор оқиғаларға әрекет ету процедураларының болуын (оқиғамен жұмыс жөніндегі процедуралар), сондай-ақ олардың «Қауіпсіздік жүйесіндегі оқиғалар туралы хабар беру» бөлімінде сипатталған хабарлау схемасына сәйкестігін тексеруі қажет.

Барлық шаралардың процедуралардың сипаттамасында дұрыс құжатталғанын, басшылық тарапынан сәйкес бақылаудың болуын, сонымен қатар оқиғалар мен жауапты шаралар жөніндегі деректер тиісті түрде тіркелетінін тексеріңіз.

6.6.1.4 Міндеттерді бөлу

Ақпараттар немесе сервистерді рұқсатсыз түрлендіру немесе орынсыз пайдалану мүмкіндігін азайту үшін міндеттерді және жауапкершілік аймақтарын бөлу жүзеге асырылуы қажет.

Аудит жүргізу жөніндегі басшылық:

Кішігірім ұйымдар үшін аталмыш мәселеде қиындықтар туындауы мүмкін: сонымен қатар, бұл бөлімде оларды қолдану үшін бөлу қағидасы ұсынылатын типтік міндеттемелер анықталады. Ірі мекемелер үшін бөліну қағидасы қалыптасқан факт болып табылады және олар процедураларды тиісті түрде айқындалған. Тәуелсіз операциялар стандартында тізімі берілген барлық салалардың ішінде қауіпсіздікті қамтамасыз ету және аудит ең маңызды болуы мүмкін және бірінші кезекте қарастырылуы тиіс.

Аудитор өңдеу кезеңдері мен шығару арасында деректер мен нәтижелердің қандай тәуелсіз тексерістер жүргізілетінін анықтауы қажет. Қатерлердің толық анализі аясында ұйым сындарлы процесстерді қарастырып, шамадан тыс тексерістер мен түзетулер үшін дара жауапкершілік көтеретін қызметкерлердің болуын анықтауы қажет. Сындарлы міндеттерге арналған жұмыс процедураларын қарастырыңыз: сырқаттануына немесе мереке күндеріне байланысты жұмысқа шықпау жағдайлары қалай шешіледі, мұндай жағдайлар операциялар тәуелсіздігіне қатер төндірме ме? Міндеттерді бөлу қағидасын тиімді түрде жүзеге асыру үшін ұйымда міндетті мерекелік кезеңдерді енгізу қажет етілуі мүмкін.

6.6.1.5 Жұмыс құралдары мен жасақтау құралдарын бөлу

Жасақтау және тестілеу құралдары жұмыс құралдарынан жеке қолдануы қажет. Бағдарламалық құралдарды бағдарлама мәртебесінен

жұмыс бағдарламасы мәртебесіне жасақтау үшін ауыстыру жөніндегі ережелер анықталып, құжатталуы қажет.

Аудит жүргізу жөніндегі басшылық:

Кішігірім ұйымдар үшін аталмыш талаптарды орындау қиынға соғуы мүмкін, бірақ жұмыс процессі кезінде іркілісті болдырмау үшін мұндай бөліністік қамтамасыз ету өте маңызды. Сәйкесінше аудитор бөлу қалай жүзеге асырылғанын және бекітудің қандай процедуралары жасақтау процессіндегі немесе тестіленбеген бағдарламалық құралдардың жұмыс жүйелерінде қолданбайтынын кепілдейтінін анықтауы қажет.

Егер жұмыс қосымшалары және ақпараттар жасақталушы және тестіленуші БҚ орналасқан компьютерлік жүйеде сақталатын болса, аудитор жаңа жасақтамалар мен жұмыс құралдарының араласуына жол бермейтін мықты басқару құралдары қолданылатынына көз жеткізуі қажет.

Жұмысшы, тестілеу жүйелері мен жасақтау жүйелері үшін әр түрлі есепке алу жазбалары мен парольдер қажет етілуі мүмкін; компиляторлар, жүйелік утилита, бағдарламаларды өңдеу құралдары және т.б. сияқты жасақтаушы аспаптары жұмыс жүйелерінен қолдануға рұқсат етілмеуі қажет. Жаңа бағдарламалық құралдар қолданысқа қалай енгізілетінін тексеріңіз және жаңа БҚ жасақтама және тестілеу кезеңінде емес екеніне көз жеткізіңіз.

6.6.1.6 Бөгде ұйымдардың әкімшілік етуі

Әкімшілік ету жөніндегі бөгде ұйымдардың қызметін пайдаланбас бұрын, қатерлер сәйкестендірілуі қажет, ал басқарудың сәйкес құралдары мердігермен келісілуі қажет; бұл ақпарат келісім-шартқа енгізілуі тиіс.

Аудит жүргізу жөніндегі басшылық:

Жүйелерге әкімшілік ету бойынша (ЖӘ) бөгде тараптардың қызметін пайдаланушы ұйымдар жоғарыда аталған талаптарды толық көлемде орындауы қажет. Қауіпсіздік жөніндегі талаптарды және басқарудың қажетті құралдарын сәйкестендіру үшін қатерлер анализін жүргізу керек, содан соң келісімді бекіту және сервистік келісімге қол қою бойынша келіссөздер жүргізіледі, ал соңында өнімділік мониторингісін жүргізу қажет.

Аудитор ЖӘ бойынша ұйымның қызметтерді пайдалануы кезінде жоғарыда аталған мәселелердің шешілгеніне көз жеткізуі қажет. Сонымен қатар, мониторинг нәтижелерін сараптау қажет: ұйым қандай жолмен маңызды және құпия ақпаратпен жұмыстың саналылығын қадағалайды? Оларда қауіпсіздік тұрғысында, сондай-ақ жұмыстың жалпы қағидалары тұрғысында олар қолданылатын ЖӘ процедуралары туралы ақпарат бар ма? Олардың жүйесіне кіруге рұқсаты бар қызметкерлер туралы олар не біледі?

5.6.2 Жүйелерді жоспарлау. Оларды қабылдау

Мақсаты: Жүйенің істен шығу қатерін азайту.

6.6.2.1 Ауыртпалықты жоспарлау

Есте сақтаушы құрылғылардың сыйымдылығы мен жүйелердің тиісті өнімділігін қамтамасыз ету үшін ауыртпалық мониторингі жүзеге асырылып, ауыртпалыққа болашақта қойылатын талаптар қатысында болжамдар жасалуы қажет.

Аудит жүргізу жөніндегі басшылық:

Ұйымдар көбіне негізгі операциялық қажеттілікті дер кезінде жоспарлауға салғырт қарайды, сондықтан аудиторлар аталмыш проблемаларды жою бойынша ұйымдардың мүмкіндігіне баға беруі қажет. Ең алдымен «Қандай параметрлерге көңіл аудару қажет?» мәселесін қарастыру қажет. Әдетте, бұл дискті жинақтағыш пен деректерді сақтаудың басқа құрылғыларының сиымдылығы, ақпаратты тарату кезінде өткізу қабілеті, принтерлерді пайдалану және басқа да мүмкін болатын «тар салалар» болып табылады. Содан соң, мониторинг көмегімен алынған ақпарат өнімділік бойынша болашақта қойылатын талаптарға баға беру үшін қалай қолданылатынын сараптау қажет. Дәстүрлі қадағалау және ағымдағы талаптарды бағамдау жұмыстағы минималды іркіліспен аппараттық құралдарды жоспар бойынша жаңартуға мүмкіндік береді. Мұнда тенденция талдаулары негізінде талап етілген өнімділік бойынша деректер алу, сондай-ақ жабдықтарды жаңарту бойынша жоспарлар мен қажеттіліктерді тексеру және сәйкестендіру кіреді. Сонымен қатар, жұмыс күшіндегі қажеттіліктерді жоспарлауды тексеру қажет. Жеткіліксіз кадрлық ресурстар сындарлы жағдайда қауіпсіздіктің бұзылуына әкелуі мүмкін.

6.6.2.2 Жүйелерді қабылдау

Жаңа ақпараттық жүйелерді, жаңарту және жаңа нұсқаларды қабылдау белгілері жасақталып, қабылдау сәтіне дейін тиісті түрде тексерілуі қажет.

Аудит жүргізу жөніндегі басшылық:

Жаңа жүйелерді енгізу немесе қазіргі уақытта қолданыстағы жүйелерді жаңарту мұқият жоспарлауды қажет етеді. Сервистердің бөгелуіне немесе жұмыс істеуші жүйелердегі деректердің әшкереленуіне жол бермеу үшін, жаңа жүйелерді енгізу, жабдықтарды жаңарту және бағдарламалық құралдардың жаңа нұсқаларын орнатудың қатаң қадағалануын жүзеге асыру қажет.

Аудиторлар жаңа жүйелерді енгізу және ескі жүйелерді жаңартуды бастамас бұрын қанағаттандырылуы қажет қабылдаудың нақты талаптарын анықтауы қажет. Жаңа жүйелер немесе процесс қолданысқа енгізілмес бұрын, олар мұқият тексерістен өтуі қажет. Қандай тестілеу жоспарлары қарастырылған, олардың саналылығы тексерілген бе, алынған нәтижелер қалайша белгіленген?

Тестілеудің жеткілікті деңгейі жаңа қызметтерді қарапайым тексеруден гөрі ауқымды шараларды қамтиды; регрессиялық тестілерге жеткілікті назар аударылды ма, пайдаланушылардың енгізу кезіндегі қателері мен дұрыс емес деректеріне жүйенің реакциясына тестілеу жүргізілді ме, қолжетімділікті бақылау тұрғысында қауіпсіздік толық қамтамасыз етілді ме, қауіпсіздік басқарудың басқа құралдары тексерілді ме?

Жүйені қабылдаумен қоса тренингтер өткізілуі мүмкін; мұндай мүмкіндік қарастырылды ма, оқыту шараларының көлемін кім анықтады, тренингті дайындау және өткізу кезінде барлық қызығушылық танытқан қызметкерлер қамтылды ма? Қолданысқа енгізуден бұрын қорытынды қабылдауға кім рұқсат береді? Аталмыш сәттер нақты анықталғанын және құжаттама түрінде бекітілгенін тексеріңіз.

6.6.3 Зиянды бағдарламалық қамсыздандырудан қорғау

Мақсаты: Ақпараттың және бағдарламалық қамсыздандырудың бүтіндігін қамтамасыз ету.

6.6.3.1 Зиянды бағдарламалық қамсыздандырудан қорғаныс құралдары

Зиянды бағдарламалық құралдардан қорғанысты қамтамасыз ететін, анықтау және алдын алу құралдары жүзеге асырылуы қажет, сондай-ақ пайдаланушыларға ақпарат беру бойынша сәйкес процедуралар жасақталуы қажет.

Аудит жүргізу жөніндегі басшылық:

Зиянды бағдарламалық құралдар барлық операциялық жүйелер үшін үлкен проблема болып табылады; сәйкесінше аудиторлар барлық қажетті басқару құралдарының адекваттығына көз жеткізуі қажет. Зиянды БҚ қорғанысының бағдарламалық құралдарын орнатудың бірнеше нұсқалары бар: кейде қорғаныс бағдарламалары серверге орнатылады және сол сәтте қосылған барлық клиенттік серверлер үшін жұмыс істейді, басқа бағдарламалар әрбір жұмыс станциясы үшін жеке орнатуды талап етеді. Жаңартуларды орнату кезінде БҚ бөлімі толық алмастырылады, ал басқа бөлімдерде жаңартулар тек белгілі кітапханалар мен базаларды ғана қамтиды; сәйкесінше аудиторлар әр нақты жағдайда бағдарламалық құралдардың ағымдағы нұсқасын қалай анықтау қажеттігін түсінуге міндетті.

Тексеруді талап ететін тағы бір маңызды сәт қажетті жаңартуды орнату тұрақтылығы болып табылады: автоматты жаңарту жүйесі қолданыла ма, әлде қорғаныстық БҚ жаңарту қажеттілігі туралы хабар беретін басқа әдіс қолданыла ма. Ықшам есептеу құрылғылары қосымша проблема туындатуы мүмкін: оларға қалайша жаңартуларды тұрақты орнату кепілден еді? Егер жаңартуларды іздестіру тұрақты түрде фондық режимде жұмыс істемесе (өкінішке орай, үнемі жүзеге асыру мүмкін емес, қалаулы нұсқалардың бірі), процедураларға нақты түрде жаңартуларды болуын тұрақты тексеру жүйесі

енгізілуі қажет. Сонымен қатар, ұйымда жүктелетін бағдарламалық құрал қатысында нақты саясат қарастырылған болуы қажет.

Ұйымда қабылданған процедуралар компьютерлік вируспен залалданған жағдайда қажетті әрекеттердің барлығын сипаттауы қажет. Зиянды бағдарламалардың барлық пайда болу фактілері тиісті түрде тіркеуге алынуы қажет. Қандай қорғаныс бағдарламалық құрал қолданылатынын тексеріңіз: ол қорғаныстың талап етілген деңгейін қамтамасыз ете ме және мұндай БҚ үшін қажетті техникалық қолдау жүзеге асырыла ма?

Тегін бағдарламалық пакеттер (мысалы, Интернет арқылы жүктеуге болатын) қажетті қауіпсіздік қорғанысын үнемі қамтамасыз етпейді, ал сирек жағдайларда қосымша шығынға ұшыратуы мүмкін. Жұмыс станцияларының операторлары қорғаныс БҚ, қосымшалар, операциялық жүйелер және т.б. дұрыс жұмыс істеу әдістері туралы мәлімденгеніне және осы әдістерді іс жүзінде қолданатынына көз жеткізіңіз: мысалы, стандартты процедурамен қарастырылмаған парольды сұрату сәйкестендіру деректерді сұрау және маңызды ақпаратты ашуға талап болуы мүмкін.

6.6.4 Жүйелерге қызмет көрсету

Мақсаты: Ақпараттық сервистердің бүтіндігін және қолжетімділігін қамтамасыз ету.

6.6.4.1 Деректерді резервке көшіру

Өндірістік қызметке байланысты маңызды ақпарат үшін, сондай-ақ бағдарламалық құрал үшін тұрақты түрде резервтік көшірмелер құрылып, тексерілуі қажет.

Аудит жүргізу жөніндегі басшылық:

Резервтік көшіру – ақпараттың бүтіндігін және қолжетімділігін қолдауға арналған негізгі компонент. Ұйымда резервтік көшіру және резервтік көшірмелермен жұмыс істеу жөніндегі шаралардың толық процедуралары қарастырылуы тиіс. Ең алдымен, резервті көшіру кезінде әрекеттердің кезектілігін тексеру қажет: ол өндірістік қызмет және қауіпсіздік жөніндегі талаптарға сәйкес болуы және ұйымның үздіксіз жұмысын қамтамасыз ету және қалпына келтіру жоспарларымен үйлесуі қажет.

Типтік желілік конфигурацияға арналған резервтік көшірме серверде орналастырылған деректер базасының толық көшірмесін, сонымен қоса бүтіндік және қолжетімділікті қамтамасыз ету жөніндегі талаптарға сәйкес берілген жиілікте (мысалы, күнделікті, апта сайын, ай сайын) жазылатын инкрементті жаңартулардың біршама мөлшерін қамтиды. Көшірменің АҚБЖ қолданысының барлық аймағын қамтитынына көз жеткізіңіз.

Сонымен бірге, резервтік көшірмелер қалай таңбаланатынын және олардың қайда сақталатынын тексеру маңызды: әрбір заттық бірлікті бір мағынада сәйкестендіруге болатынын, ол туралы деректер тиісті түрде

тіркелгеніне және сақтаудың қауіпсіз жағдайлары қамтамасыз етілгеніне көз жеткізіңіз. Резервтік көшірмелері бар таратушылардың және осы деректер алынған жүйелердің сақталатын орны әр түрлі жерде орналасуы қажет; сонымен қатар, негізгі деректерге сияқты дәл сондай қауіпсіздік деңгейін резервтік көшірмелерге қамтамасыз ететін басқару құралдары жүзеге асырылуы тиіс.

Сындарлы деректерді ұзақ мерзім сақтауға қандау талаптар қойылатынын, осы талаптардың сақтауын ұйымда қалай қадағалайтынын анықтаңыз – резервтік көшірмелер жазылған таратушылар өздігінен тозуы және алмастыруды талап етуі мүмкін. Сондай-ақ, резервтік көшіру процедураларды қарастыру қажет, көшіру жасалу мүмкін болмаған жағдайда қандай түзету шаралары қарастырылған, деректерді қалпына келтіру қалай ұйымдастырылған, мұндай қалпына келтіру шаралар қандай жиілікте жүргізіледі, барлық жүзеге асырылатын шаралар қалай тіркеледі. Резервтік көшірмелері бар таратушылардың қызмет ету қабілеті тестілене ме? Резервтік көшірмелерден деректердің тестілік қалпына келтірілуі ақпарат бүтіндігін бұзбауы қажет; аталмыш талаптар тиісті түрде ескерілгеніне көз жеткізіңіз. Ұйымның үздіксіз жұмыс істеуін қамтамасыз ету талаптары резервтік көшірмелердің қолжетімділігі, ақпарат тартушылардың сенімділігі, жиілік тұрғысында сақталатынын тексеріңіз.

6.6.4.2 Операторлар әрекетінің және қателерді тіркеу журналы

Жүйелерге қызмет көрсетуші қызметкерлер өз әрекеттерін тіркеу журналын жүргізуге міндетті. Операторлар әрекеттерінің журналы тұрақты түрде тәуелсіз тексерістен өтуі қажет.

Қателіктер туралы ескертулер жасалып, сәйкес түзету шаралары жасалуы қажет.

Аудит жүргізу жөніндегі басшылық:

Компьютерлермен жұмыс жөніндегі операциялық процедураларда қалыпты жұмыс барысында, сондай-ақ кемшіліктер болған жағдайда қандай журналдар жүргізілуі қажет екені көрсетілуі қажет. Ішкі мониторинг аясында журналдарда талдау куәлігі айқындалуы қажет. Ұйым жұмысының барысындағы операторлар әрекетінің журналын тексеру кезінде онда ауысымдық жұмыс, жұмысты тапсыру жөніндегі операциялар, ерекше талаптар және т.б. қалай көрсетілгенін тексеріңіз. Сонымен қатар журналдарды (автоматты түрде құрылатын, сондай-ақ қолмен жүргізілетін) мұрағатқа тапсырылуына назар аударыңыз: мұндай журналдар қалай таңбаланады, оларды қалайша алуға болады.

Журналдардағы жазбалар бойынша әрбір кемшілік тұстары бойынша адекватты түзету жұмыстарының орындалу фактісін аңдау мүмкін болуы қажет. Талдау белгілеріне қауіпсіздіктің бұзылуының болмауын тексеру кіруі қажет; бұл сәйкес процедураларда қамтылғанын және басшылық қаперіне жеткізілгенін тексеру қажет. Кемшіліктері бар барлық

жағдайлардың адекватты шешімін табуды қамтамасыз ету қажет. Сонымен қатар, аудиторлар кез-келген түзету шараларының тек сәйкес рұқсат болған жағдайда ғана жүзеге асырылатынын тексеруі қажет.

6.6.5 Желістік әкімшілік

Мақсаты: желіс арқылы таратылатын ақпараттың және қолдаушы инфрақұрылымның қорғанысын қамтамасыз ету.

6.6.5.1 Желісті басқару құралдары

Желіс арқылы таратылатын ақпараттың қауіпсіздігін қамтамасыз ету үшін бірқатар басқару құралдары жүзеге асырылуы қажет.

Аудит жүргізу жөніндегі басшылық:

Желіс, сондай-ақ қызмет ету ортасының топологиясы, әсіресе маңызды ақпараттың таратылуы барысында, тиісті түрде жоспарланып, әкімшілік жасалуы қажет; басшылықта мұны формальды түрде растаушы құжаттардың бар екеніне көз жеткізіңіз. Ішкі желістер ашық желістерге кіру мүмкіндігі болған жағдайларға тиісті назар аударылды ма, немесе олардың инфра құрылысы пайдаланылды ма және сәйкес қорғаныс механизмдері жүзеге асырылды ма?

Үлкен, күрделі жобалар үшін кеңесші-мамандардың қызметтері қажет етілуі мүмкін. Егер кеңесшілер қызметке тартылмайтын болса, желістерді тарату жөніндегі ішкі мамандардың дайындық деңгейін мұқият тексеріңіз. Желістік операциялардың ең осал тұстары анықталды ма және қандай қорғаныс шаралары қолданды? Желістердегі қауіпсіздіктің бұзылуы үнемі дереу анықтала бермейді; деректердің ұрлануы, олардың көшірілуі немесе түрлендіру ешбір іздерсіз жүргізілуі мүмкін.

Мониторингтің қандай құралдары қауіпсіздіктің мұндай бұзылуын анықтау үшін қолданылатынын тексеріңіз, және аталмыш жағдайларда қолданылатын тиісті әрекеттер оқиғалар туралы мәлімдеу жөніндегі процедураларда сипатталғанына көз жеткізіңіз. Желістер, деректерді шифрлау, сандық қолтаңбалар және т.б. – бұл технологиялар қарқынды дамитын салалар болып табылады; ұйым осы салалардағы жаңа жетістіктерді қалай қадағалайтынын және қауіпсіздіктің жаңа қатерлерін идентификациялап олардың пайда болу шамасына қарай сәйкес механизмдерді қалай қолданатынын анықтаңыз.

6.6.6 Ақпаратты таратушыларды басқару және оларды қорғау

Мақсаты: Ақпараттық ресурстардың зақымдалуын және ұйым жұмысының бөгелуін болдырмау.

6.6.1.1 Ақпараттың алынбалы таратушыларын басқару

Магнитті таспалар, дисктер, кассеталар және қағазға басылған есептер сияқты ақпараттың алынбалы таратушыларын басқару қадағалануы қажет.

Аудит жүргізу жөніндегі басшылық:

Ақпараттың алынбалы таратушылары ұйым аймағынан тыс қалай алынып шығарылатынын анықтаңыз. Таратушыларды мұрағатқа жеткізу үшін, қызметкерлердің жұмыс бабында пайдалануы үшін немесе жою үшін олар сыртқы шығарылуы мүмкін. Бұл жағдайлардың әрқайсы үшін сәйкес процедура мен тіркеу тетігі қарастырылуы қажет. Мұндай процедура ақпараттар ағынын болдырмауды кепілдеу үшін алынбалы таратушылардың деректерден тазартылуын қамтамасыз етуі қажет. Егер таратушы жойылатын болса немесе қандай да бір басқа себептермен бағалы ақпаратты сақтау үшін ары қарай қолданылмайтын болса, онда сақталатын деректер қалай өшірілгенін және таңбалануы қалай жойылғанын және т.б. тексеріңіз.

Сонымен қатар, әр түрлі таратушыларға арналған тасымалдау процедураларын қарастырған жөн: олар жеткілікті қорғаныс деңгейін қамтамасыз ете ме? Басқарудың қандай да бір құралдары қолданылмасын, бұл саладағы бақылау өте күрделі, сондықтан ұйым тәуекелдерді бағалау кезінде бұл жағдайды ескерді ме, бұл басқарудың қосымша құралдарын қолданумен өте ме деген сұрақтарды қарастыру қажет.

6.6.6.2 Ақпараттарды таратушыларды жою

Енді қажеті жоқ ақпарат таратушыларды жою қауіпсіз әрі сенімді әдіспен жүзеге асырылуы қажет.

Аудит жүргізу жөніндегі басшылық:

Жойылуы тиісті немесе балама пайдалануға жататын таратушылардағы ақпаратты өшіру жоғарыда қарастырылған.

Жою жөніндегі жалпы процедуралар қандай екенін, бөгде тараптық мердігерлер қызметі пайдаланылу мүмкіндігін анықтаңыз, ұйым басқа процесстермен қарастырылған тексеріс және қауіпсіздіктің қажетті тексерістерін орындағанына көз жеткізіңіз және мұндай процедураларға қатысы бар ақпарат құпиялылығының максималды деңгейі қамтамасыз етілгенін қадағалаңыз. Процедуралар қаншалықты нақты болғанымен таратушыларды жою процессінде бағалы ақпарат алдын ала өшірілген немесе жойылғандықтан мұндай құнды ақпараттың әшкереленуі мүмкін еместігіне көз жеткізу қажет. Жою жөніндегі шаралар үшін қандай да бір түрдегі есептілік қарастырылуы қажет; оның ары қарай бақылау жүргізу үшін жеткілікті ақпарат беретініне көз жеткізіңіз.

6.6.6.3 Ақпаратты пайдалану процедуралары

Ақпаратты рұқсатсыз ашу немесе пайдаланудан қорғау үшін осы ақпаратты пайдалану және оны сақтау бойынша процедуралар жасақталуы қажет.

Аудит жүргізу жөніндегі басшылық:

Аудиторлар ұйымда қабылданған жіктеу схемасына сәйкестікте маңызды ақпаратты (оның қандай пішінде ұсынылғанына тәуелсіз) қорғау

бойынша процедуралардың болуына көз жеткізуі қажет. Ақпаратқа жауапты тұлғалар құжаттарда қалай белгіленеді, оны тарату үшін қалайша рұқсат алу қажет?

Ақпаратты қызметкерлерге белгісіз тұлғалар (курьерлер сияқты) пайдаланған жағдайда, тұлғаны қосымша тексеру шаралары жүргізіле ме? Олардың қолжетімділігін шектеу жүзеге асырылған ба, егер иә болса, нақты қандай шаралар жүзеге асырылған?

6.6.6.4 Жүйелік құжаттаманы қорғау

Жүйелік құжаттама рұқсатсыз ашу мүмкіндігінен қорғалуы қажет.

Аудит жүргізу жөніндегі басшылық:

Жүйені пайдалану жөніндегі нұсқама, баптау және конфигурация жөніндегі деректер, қолжетімділік құқығының тізімі сияқты құнды және құпия ақпараттар үшін құжаттармен жұмыс жөніндегі стандартты процедуралардың кеңейтілуі мүмкін. Мұндай жүйелік құжаттама маңызды және құпия ақпаратты қамтуы мүмкін. Аудиторлар қауіпсіздік классификациясының жүйесі оларға дұрыс қолданылатынына және құжаттар тиісті түрде таңбаланғанына көз жеткізуі қажет.

Мұндай құжаттама өндірушілердің өзімен ұсынылатын жағдайлардың болуы әбден мүмкін, және сәйкесінше проблемаларды жою сыртқы тарапты дереккөзден түскен деректер негізіне сүйенеді. Жабық құжаттарды беру және тарату бұл мүмкін болған жерде қатаң түрде қадағалануы қажет; Бірқатар жағдайларда көшіру қажет болуы мүмкін. Егер жүйелік құжаттама желістік ресурстарда орналастырылған болса, мұндай құжаттамаға тек уәкілетті қызметкерлердің пайдалануына рұқсат беруші қолжетімділікті басқарудың адекватты құралдары жүзеге асырылуы қажет.

6.6.7 Ақпараттармен және бағдарламалық құралдармен алмасу

Мақсаты: Ұйымдар алмасатын ақпараттың жоғалуын, түрлендірілуін және рұқсатсыз пайдалануын болдырмау.

6.6.7.1 Ақпаратпен және бағдарламалық құралдармен алмасу жөніндегі келісім

Ұйымдар арасында ақпаратпен және бағдарламалық құралдармен алмасу (электронды әдіспен немесе қолдан қолға) жөніндегі, кейбірі формальды болуы мүмкін келісімдер жасақталуы қажет.

Аудит жүргізу жөніндегі басшылық:

Аудиторлар ең алдымен қандай ұйымдардың құпия ақпаратпен алмасуға қатысатынын анықтауы қажет, содан соң келісім-шарттық міндеттіліктерді бекітуші құжаттардың болуына көз жеткізуі қажет. Бұл жерде ақпарат, сондай-ақ, бағдарламалық құрал ұғымдары өз мәнінде қолданылады. Мұндай жағдай БҚ өндіруші-компания сындарлы деректерді пайдалануға арналған бағдарламаларды жасақтағанда туындауы мүмкін;

ұйымға үшінші тараптардан депонирлеу туралы келісім арқылы осы бағдарламалық құралға қолжетімділікті қамтамасыз ету қажет етілуі мүмкін.

Басқа ұйымдардың қарамағындағы ақпарат үшін қандай қорғаныстыұсынатынын қарастырыңыз.

6.6.7.2 Ақпараттарды тасымалдау кезінде оларды қорғау

Тасымалданатын ақпаратты таратушылар рұқсатсыз ашылудан, құқықсыз пайдалану немесе зақымдалудан қорғалуы қажет.

Аудит жүргізу жөніндегі басшылық:

Ақпараттың физикалық тасымалдануы жүргізілетін барлық жағдайларда осы ақпарат орналастырылған таратушылардың қорғанысы қалай жүзеге асырылатыны туралы ойлану қажет. Тасымалдау қалай ұйымдастырылған? Егер курьерлық қызмет көмегімен болса, қорғаныс, соның ішінде рұқсатсыз ашудан қорғалған контейнерлер ұсынылама? Деректер қызметкерлермен дискте немесе таспаларда немесе алып жүретін компьютерлерде өткізіле алады; таратылатын деректер үшін мұндай әдіс жеткілікті түрде қауіпсіз бе?

Тасымалдау әдісін кім анықтайды, ал бұл тұлғалар қандай талаптарды ұстанады? Курьерлық қызметті қолдану кезінде тасымалдау әдістері жөніндегі мәселе өздігінен шешіледі және тасымалдауды стандартты жағдайларда пайдалану мүмкіндігі туады – қауіпсіздіктің жеткілікті деңгейі қамтамасыз етіле ме? Сонымен қатар поштамен жеткізілу мүмкіндігін қарастыру қажет, ол қауіпсіз болып табыла ма? Қорғалатын ақпараттың тасымалдануы қажет етілетін барлық жағдайларда жеткізілімнің қалай ұйымдастырылатынын анықтаушы процедуралар қарастырылуы қажет, тасымалдауға қажетті рұқсаттар нақты көрсетілуі қажет, ал олардың болуы құжат түрінде бекітілуі қажет.

6.6.7.3 Электронды коммерция жүйелерін қорғау

Электронды коммерция жүйесі алаяқтар әрекетінен, әрекеттерді даулау мүмкіндігінен және ақпаратты ашу немесе түрлендіру мүмкіндігінен қорғалуы тиіс.

Аудит жүргізу жөніндегі басшылық:

Аудиторлар электронды коммерция пайдаланылған ұйымның ағымдағы және болашақтағы операциялар туралы анықтамалар жүргізуі қажет. Ұйымның электронды коммерцияға байланысты барлық қызметі қауіпсіздік мәселесі ауқымында сарапталуы қажет. Мұнда келесі тексерістер қамтылуы қажет:

– Авторизация процессінің болуы: электронды коммерция жүзеге асырылатын операциялар ұйымның тек авторизацияланған қызметкерлерімен жүргізіле ала ма;

– Міндеттердің тиісті түрде бөлінуі: жиынтығында алаяқтық мақсатта қолданыла алатын әрекеттер бөліне ме және олардың үстінен бақылау жүргізіле ме;

– Электронды транзакцияға байланысты өңделетін, ақпараттың ақиқаттылығын, бүтіндігін және құпиялығын қамтамасыз етуге мүмкіндік беруші, сәйкес криптографиялық басқару құралдарының болуы, сондай-ақ мұндай басқару құралдарының қолданысын реттеуші саясаттың жүргізілуі;

– Басқа желістермен қосылудан туындауы мүмкін шабуылдардан электронды коммерция үшін қолданылатын ұйымның желісінің және желіс торабының қорғанысын қамтамасыз етуші, желістік қауіпсіздіктің сәйкес басқару құралдарын жүзеге асыру;

– Сырттан келетін қатерден жеткілікті қорғаныстың болуы.

6.6.7.4 Электронды поштаны қорғау

Электронды поштаны қолдануға байланысты қауіпсіздіктің бұзылу қатерін азайту үшін электронды поштаны пайдалану саясаты жасақталуы қажет және қажетті бақылау шаралары қолдануы қажет.

Аудит жүргізу жөніндегі басшылық:

Бүгінгі күні электронды пошта арқылы хат-хабарлармен алмасу барлық ұйымдарда кеңінен тараған. Электронды пошта өте әлсіз болғандықтан, оның қорғанысы үшін қолданылатын басқару құралдарын мұқият зерттеу қажет: хабар мәтінінде мазмұндалған және файлдарға тіркелген ақпарат қалай қадағаланады, жеткізу дұрыстығы қалай тексеріледі? Электронды пошта арқылы жеткізілетін дереккөздері және деректердің бүтіндігі қалай тексеріледі?

Егер ұйымда криптографиялық қорғаныс құралдары қолданылатын болса, олар нақты қандай? Электронды пошта арқылы келіп жеткен ақпарат вирустардың болу мүмкіндігіне пайдаланбас бұрын тексеріле ме? Ұйым ішінде таратылатын, электронды поштаның хаттары сыртқы адресаттармен жіберілетін хаттармен салыстырғанда ерекше бүтіндік мәртебесіне ие ме? Егер иә болса, олар қандай жолмен анықталады және қадағаланады?

Электронды поштаны пайдалану сот дауларының едәуір қатеріне байланысты, және ұйымда аламыш жағдайға нақты жасақталған және жүзеге асырылған саясат болуы қажет. Ішкі хаттар абайсызда сыртқы адресаттарға жіберілуі мүмкін, өзіне аңдаусызда келісім-шарттық міндеттемелер арту қатері бар, хаттар және тіркелген файлдар жылдар бойы резервтік көшірмелерде сақтала алады. Хаттар мәтініне енгізілетін, жауапкершіліктен бас тарту жөніндегі стандартты ереже көмектесуі мүмкін, бірақ қорғаныс құралы ретінде олардың құқықтық мәртебесі күмәнді болып табылады.

Аудиторлар әсіресе, электронды корреспонденцияның сыртқы адресаттарға жіберілуі рұқсат етілген кездері ұйыммен сәйкес тәуекелдердің бағалануы жүргізілгеніне және оның нәтижелері ескерілгеніне көз жеткізуі

қажет. Мысалы, қорғаныс шарасы ретінде электронды поштаны қызметкерлердің шағын тобына ғана қолдануға мүмкіндік беруші шектеу енгізілуі мүмкін. Егер мұндай шектеу қолданылған болса, оның орындалуы қалай қамтамасыз етіледі? Қолданылған қорғаныс механизмін тестілеп көріңіз.

6.6.7.5 Электронды офис жүйелерін қорғау

Электронды офис жүйелерін пайдалануға байланысты қауіпсіздік жүйелері мен өндірістік процесстерге төнуі мүмкін қатерлерді бақылау үшін сәйкес саясаттар мен ұсыныстар дайындалып, жүзеге асырылуы қажет.

Аудит жүргізу жөніндегі басшылық:

Электронды офис жүйелерін қолдану өнімділіктің едәуір ұлғаюына мүмкіндік берсе де, онымен қатар дұрыс қарастырылмаған жұмыс процедуралары салдарынан өңделетін ақпараттың құқықсыз пайдалану, ашылу немесе жойылу қатері де солғұрлым өседі. Аудиторлар қандай процедуралардың жасақталғаны, олар қалайша жүзеге асырылғанын, қандай ақпаратты қайда сақтау керек екенін және қайда болмасын сәйкес қатерлер қарастырылғанын анықтау қажет.

Істерді жоспарлаудың электронды жүйелерін пайдалану бұл ақпарат олар үшін арналмаған тұлғалар арасында басшылықтағы негізгі фигуралардың алмастырылуы туралы деректердің мен жабық ақпараттардың таралуына әкелуі мүмкін; жалпыға ашық қызметкерлер жөніндегі деректер базасы құпия жеке ақпаратты қамтуы мүмкін; құжаттар айналымын басқару пакеттері енгізілген кезде жіберілген немесе зақымдалған немесе жеткілікті түрде уәкілетті емес немесе сәйкес рұқсаты жоқ қызметкерлермен енгізілген деректерге өз жұмысын негіздей алады.

Жолданатын ақпарат және осы жүйелерге қолжетімділікті бақылануына талдау жасаңыз. Пайдаланушылар олар жолдайтын ақпараттарды офистік жүйеге ашық кіре алатын кез-келген тұлға оңай аша алатынын біле ме?

Электронды офис құралдарына сырттан кіру мүмкіндігіне рұқсат берілген жағдайларда (мысалы, қызметкерлер үйде жұмыс жасағанда немесе басқа ұйымдармен әрекеттесу кезінде) сыртқы қосылыстар жалпы желістің қауіпсіздік деңгейін едәуір төмендетуі мүмкін және қосымша басқару құралдарын пайдалану мүмкіндігі қарастырылуы қажет. Интернет сияқты ашық қол жетімдігі бар желіс арқылы қосылу кезінде бұл мәселе ерекше маңызға ие болады.

6.6.7.6 Жалпыға ашық жүйелер

Ақпаратты ашық жүйеге орналастыру формальды процедура аясында рұқсат етілген болуы қажет және бұл ақпараттың бүтіндігі рұқсатсыз түрлендірудің алдын алу үшін қорғалған болуы қажет.

Аудит жүргізу жөніндегі басшылық:

Егер ақпаратты жариялау үшін, сондай-ақ деректер мен ақпараттарды алу үшін аталмыш ұйымдарда Интернет желісіне қосылған Web-сервер сияқты ашық кірісі бар жүйелер қолданылатын болса, аудиторлар қауіпсіздікті қорғау үшін қандай басқару құралдары қолданылатынын анықтауы және олар дұрыс жүзеге асырылғанын тексеру қажет.

Мұнда ақпаратты жариялау үшін қажетті болып табылатын бекіту процессін тексеру кіреді. Қызметкерлер жаңа Web-беттер қоса ала ма немесе сәйкес рұқсат алмай жарияланған ақпараттарға өзгертулер енгізе ала ма? Жарияланған ақпараттың мазмұнын тұрақты тексеру міндетіне кіретін қызметкерлер ұйымда қарастырылған ба? Қызметкерлердің бірі қолданыстағы заңнама нормаларына, әсіресе ақпарат ашық жүйеде орнатылған елдің заңнамасына сәйкестікке ашық жүйе көмегімен жарияланған немесе алынған ақпаратты тексерді ме? Жарияланған ақпарат сырттан манипуляциялау мүмкіндігінен қорғалды ма?

Жарияланған ақпаратты қорғауды қамтамасыз етумен қоса, рұқсатсыз қолжетімділікті алу мақсатында жариялану үшін қажетті қосылыстарды пайдаланушы басып кіруден корпоративті желісті қорғау қажет етілуі мүмкін. Аудиторлар мұндай рұқсатсыз кіруден қорғау үшін басқару құралдарының жүзеге асырылғанын тексеру қажет.

6.6.7.7 Ақпаратпен алмасудың басқа формалары

Дыбыстық байланыс, факсимильді байланыс және бейне мәслихат құралдарының көмегімен жүзеге асырылатын ақпаратпен алмасудың қорғанысын қамтамасыз етуші басқару құралдары мен процедуралары, саясаттар жасалуы қажет.

Аудит жүргізу жөніндегі басшылық:

Аталмыш басқару құралы мобильді есептеу құрылғыларын, стационарлы және ұялы телефондарды, факс аппараттарын, қалталы компьютерлер, автожауап қабылдағыш және т.б. қолдану кезінде қауіпсіздікті қамтамасыз етуге қатысты. Аудиторлар қандай процедуралар ақпараттық айырбастың аталмыш түрін басқару үшін жасақталғанын анықтауы және олардың басқару құралдарына сәйкестігін тексеруі қажет.

Қызметкерлер аталмыш процедуралар қатысында хабардар болғанына көз жеткізу қажет. Мұны мысалы, олардың мобильді телефондарын, авто жауап қабылдағыш немесе факс аппараттарын қалай пайдаланатынын сұрастыру және мұндай қолданысқа байланысты қатерлер туралы мәлімденгенін анықтау арқылы білуге болады.

6.7 Қолжетімділікті басқару

6.7.1 Қолжетімділікті басқаруға қойылатын өндірістік талаптар

Мақсаты: Ақпаратқа қолжетімділікті басқару.

6.7.1.1 Қолжетімділікті басқару саясаты

Қолжетімділікті басқаруға қойылатын өндірістік талаптар нақты анықталып, құжатталуы қажет, жүйеге кіру мүмкіндігі қолжетімділікті басқар саясатына сәйкес шектелуі қажет.

Аудит жүргізу жөніндегі басшылық:

Аудиторларға қолжетімділікті басқару саясатын анықтаушы, құжаттағы қолжетімділік құқығының нақты анықтамасын қамтамасыз ету қажет және осы саясаттың талаптарын қамтамасыз ету бойынша жүзеге асырылған механизмдердің болуына көз жеткізу қажет. Құпия ақпаратқа кез-келген қолжетімділік қажеттілік қағидасына негізделуі қажет: ақпаратты пайдалану құқығы өндірістік талаптарға сәйкес және жұмыстарды орындау үшін аталмыш ақпараттардың қажеттілігі болған жағдайда берілуі қажет.

Егер қажеттілік қағидасының сақталуы күмәнді бола, аудиторлар қызметкерлердің (бірқатар жағдайларда – ұйымның жоғарғы басшылығы санатынан) белгілі ақпаратты пайдалану құқығы бар себептерін анықтауға дайын болуы қажет. Маңызды және құпия ақпаратқа қолжетімділік қорғаныс классификациясына сәйкес жүргізілгенін және мұндай ақпаратты пайдалану құқығы бар қызметкерлер тиісті түрде нұсқама алғанын тексеріңіз. Құпия ақпаратты біліктілігі жоқ қызметкерлердің қадағалаусыз пайдалануы күрделі салдарға әкелуі мүмкін.

6.7.2 Пайдаланушылар қолжетімділігін басқару

Мақсаты: Қолжетімділік құқығын тиісті түрде бекіту, тағайындау және қолдауды қамтамасыз ету.

6.7.2.1 Пайдаланушыларды тіркеу

Барлық көпшілікпен пайдаланылатын ақпараттық жүйелер мен сервистерге қолжетімділікті басқару үшін пайдаланушыларды тіркеудің және пайдаланушылардың есеп жазбасын өшірудің формальды процедурасы болуы қажет.

Аудит жүргізу жөніндегі басшылық:

Пайдаланушылардың қолжетімділігін формальды басқару мен тіркеуді қамтамасыз ету қажет. Жоғарыда қарастырылған саясаттарға сәйкес, аудиторлар барлық пайдаланушылардың қолжетімділік деңгейі авторизация мен тіркеудің формальды процессі негізінде жүргізілетінін, ал қолжетімділік фактілері тіркелетінін кепілдеуі қажет. Мұндай тіркеу жазбалары шындыққа сай келетінін тексеріңіз; қызметтен босатылған және басқа міндеттер алған қызметкерлер сәйкес тізімнен шығарылды ма?

Көптеген жағдайларда аудиторлар қолжетімділік тек тіркелген және сәйкес авторизациядан өткен пайдаланушылар үшін ғана рұқсат етілегіне көз жеткізу мақсатында нақты топтар мен жекелеген пайдаланушылар үшін қолжетімділік құқығын анықтаушы операциялық жүйелерің бапталуын зерттеу үшін жүйелік әкімгерлермен жұмысқа едәуір уақыт бөлуге тура келеді.

6.7.2.2 Артықшылықтарды басқару

Артықшылықтарды беру және олардың қолданылуы шектеліп, қадағалануы қажет.

Аудит жүргізу жөніндегі басшылық:

Анықтамалар бойынша ерекше артықшылықтар қарапайым жағдайда қолданысы шектелген жүйелік қызметтерді пайдалану мүмкіндігін береді. Жүйелік әкімгерлерге, жүйелік инженерлерге және жабдықтар мен бағдарламалық құралдарды жеткізуші инженерлерге, сондай-ақ қызметтері жүйелерге артықшылықты қолжетімділікті білдіретін барлық қызметкерлерге ерекше назар аударыңыз. Қолжетімділіктің бұл деңгейі шектеулі болуы қажеттігіне қарамастан, артықшылықты қолжетімділік құралы бір қызметкерде ғана емес, көптеген қызметкерлерде бар екеніне көз жеткізіңіз, себебі сәйкес мониторингсіз жүргізілетін әрекеттерді бақылау мүмкіндігі мен қолжетімділік зиян шегуі мүмкін.

Қорғалған ақпаратқа қолжетімділік, сонымен қатар, сейфтік құлыптар мен басқа да қорғалған салалардың кодтарын қамтуы мүмкін; мұндай кодтар сәйкес түрде тіркеліп, белгілі кезеңдікте алмастырылуы қажет. Ақпараттың қолжетімділігі тек бір ғана қызметкерде қолжетімділік құқығының болуына байланысты зиян шекпейтініне көз жеткізу қажет. Сонымен қатар, артықшылықтар қажеттілік қағидасына сәйкес ұсынылатынын және ол қажеттілік күшін жоғалтқан әрбір нақты жағдайда артықшылықтың жойылатынын және оның қалыпты еңбек қызметі аясында қолданбайтын ерекше есеп жазбасымен қауымдасатынын тексеру қажет.

6.7.2.3 Пайдаланушылардың парольін басқару

Парольдерді тағайындау формальды басқару процессінің көмегімен бақылануы мүмкін.

Аудит жүргізу жөніндегі басшылық:

Парольдерді бақылау артықшылықты қол жетімдік мәселелерімен тығыз байланысты; бұл авторизацияланған пайдаланушыларға арналған қолжетімділікті қамтамасыз етудің негізгі (бірақ дара емес) тетігі. Парольдердің қалай тағайындалып, бақыланатынын біліңіз: кейде бұл мәселені пайдаланушының өзі шешеді, басқа жағдайларда парольдер жүйелік администраторлармен құрылып, тағайындалады. Егер парольдерді тағайындау орталықтандырылған болса, парольдер қайда сақталады, қауіпсіздік қорғанысы қамтамасыз етілген бе, парольдер қорына кім кіре

алады? Парольдерді тағайындау процессі қандай да болмасын, ол пайдаланушының бір мәнді сәйкестендіру қағидасына негізделуі қажет және пайдаланушының бастапқы, уақытша паролын тұрақтыға ауыстыруын талап етуші формальды процедураны қарастыру қажет. Пайдаланушылардың парольді құпияда сақтау жөніндегі міндеттілігіне қол қойғанына және олар оның орындалуы үшін жауапкершілікті түсінетінін тексеріңіз.

6.7.2.4 Пайдаланушылар қолжетімділігі құқығын қарастыру

Басшылық пайдаланушылардың қолжетімділік құқығын қайта қарастырудың формальды процессін тұрақты түрде орындауы қажет.

Аудит жүргізу жөніндегі басшылық:

Қолжетімділігі құқығын тұрақты қайта қарастыру және жаңартусыз жай ғана тағайындау қауіпсіздікті қамтамасыз ету үшін жеткіліксіз. Аудиторлар пайдаланушыларға арналған барлық қолжетімділік құқықтарының түрін тұрақты түрде қайта қарастыру бойынша процедуралардың болуына және олардың қолданылуына көз жеткізуі қажет. Бұл процедуралар кауіпсіздік саясаты талаптары мен өндірістік талаптармен үйлесімділікті тексеру үшін басшылық тарапынан қолжетімділік құқығын қайта қарастыру жүргізілетін сәйкестікті тексеруге арналған формальды аудитты қамтуы мүмкін.

Жағдайлар өзгергенде, қызметкерлер босатылғанда және жұмысқа қабылданғанда, қызметтік міндеттердің өзгеруі, жүйенің дамуы кезінде жекелеген пайдаланушылардың қолжетімділік құқықтары тиісті түрде қадағаланып, жаңа талаптарға сәйкес келуін қамтамасыз ету өте маңызды. Ерекше артықшылықтар үшін қосымша бақылау шаралары қарастырылғанына көз жеткізіңіз (мысалы, жоспардан тыс немесе нақты тексерістер).

6.7.3 Пайдаланушылардың міндеттері

Мақсаты: Пайдаланушылардың рұқсатсыз кіруін болдырмау.

6.7.3.1 Парольдерді пайдалану

Парольдерді таңдау және пайдалану кезінде пайдаланушылар қауіпсіздік режимін қолдаудың бекітілген процедураларын басшылыққа алуы қажет.

Аудит жүргізу жөніндегі басшылық:

Парольдерді ауыстыру жөніндегі саясат (алмастыру жиілігі, минимальды ұзындығы және пароль құрамына қатысты) қауіпсіздікті қорғау бойынша ақпараттық талаптар мен ұйым талаптарына сәйкес болатынын тексеріңіз. Кейбір жүйелерде парольдерді тағайындау ережелері міндетті түрде қарастырылған, басқаларында олар қарастырылмаған – егер мұндай ережелер автоматты түрде қолданылмайтын болса, қандай қосымша шаралар қарастырылған. Қажет болған жағдайда қызметкерлерден олардың

парольдерін қалай алмастыратынын көрсетуін өтініңіз – олар парольді таңдау белгілерімен таныс па, олар қолданатын кодтар ұйымда қабылданған саясатқа сәйкес келе ме?

Сонымен қатар, парольдер қолжетімділігі оңай жерлерде (блокноттарда, мониторларға жапсырылған жапсырмаларда және т.б.) жазылғанын тексеріңіз. Қосымша мәліметтерді жоғарыда мазмұндалған «Пайдаланушылар парольдерін басқару» бөлімінен, сондай-ақ мәтін бойынша сілтемелер жасалған басқа бөлімдерден алуға болады. Ұйымдағы парольдерді пайдалану тексерісі кезінде аудиторлар басшылықтың сәйкес рұқсаттарын алуға тиісті.

6.7.3.2 Қараусыз қалдырылған пайдаланушы жабдығы

Пайдаланушылар қараусыз қалдырылатын жабдықтың тиісті қорғанысын қамтамасыз етуге міндетті.

Аудит жүргізу жөніндегі басшылық:

Аудит тұрғысында мұнда ең бастысы – процедуралардың болуы, қызметкерлердің төнуі мүмкін қатерлер мен талаптардың мән-жайын білуі, сондай-ақ қабылданған процедураларды орындауын қамтамасыз ету. Ұйымда қараусыз қалдырылған, сөндірілмеген және парольмен қорғалмаған терминалдардың болуын байқаңыз. Дербес компьютерлердегі экран сақтағыштар да парольмен қорғалған болуы қажет - бұл талаптың орындалуын қадағалаңыз. Кез-келген сөндірілген терминалдарды қосуды өтініңіз – ақпарат рұқсатсыз пайдаланудан қорғалған болуы қажет.

Желістік серверлер, коммуникациялық жабдықтар және т.б. сияқты қауіпсіздіктің жоғары талаптары қойылатын, автономды режимді штатты түрде жұмыс істейтін жабдықтар қорғалған жерде орналастырылуы қажет - бұл талап орындалғанына және қорғаныстың жеткілікті шаралары қолға алынғанына көз жеткізіңіз.

6.7.4 Желіске кіру мүмкіндігін басқару

Мақсаты: Желістік сервистердің қорғанысын қамтамасыз ету.

6.7.4.1 Желістік сервистарды пайдалану саясаты

Пайдаланушылар оларға қолдануға анық рұқсат етілген сервистерге ғана тікелей кіруге рұқсат алуы қажет.

Аудит жүргізу жөніндегі басшылық:

Терминал немесе қосымшаға енуші пайдаланушы оған қолдануға рұқсат етілген және оның қызметтік міндеттерін орындау үшін қажетті сервистер мен ақпараттарды пайдалану мүмкіндігіне ғана ие болуы қажет. Мысал ретінде келесі жағдайды қарастыруға болады деректер базасындағы қолжетімділік аясында терминал пайдаланушысы тек тренингтен өтуі жөніндегі жеке деректерді қарай алады, ал сол деректер базасындағы жалақы жөніндегі жеке мәліметтерді пайдалану мүмкіндігіне құқығы жоқ. Қандай да

бір пайдаланушының нақты қандай қолжетімділікке ие болатыны айқын анықталуы қажет:кебір қосымшалар үшін барлық ақпаратқа қолжетімділік еш қиындық туғызбайды, ал сол мезетте басқа қосымшалар үшін мұндай жағдай күрделірек болуы мүмкін. Қолжетімділікті тек құпиялыққа байланысты шектеу қажет емес; мұнда мәселе ақпарат бүтіндігін бұзу немесе белгілі ақпаратты пайдалану кезінде басқа деректердің өздігінен әшкереленуінде болуы мүмкін.

Аудитор талап етілген шектеулер қолжетімділікті қадағалау саясатына сәйкес жүзеге асырылғанына және сәйкестендірілгеніне, аталмыш шектеулер басшылықтарға мәлім екеніне, қолжетімділік құқықтары қосымша баптаулары мен дизайнына енгізілгеніне, және де қолданылған құралдар тиімді болып табылатынына көз жеткізуі қажет. Сонымен қатар, қызметкер терминалдан негізгі сервер немесе есептеу торабына қосылған жағдайда операциялық жүйе деңгейінде қолжетімділікті зерттеңіз. Дирекция құрылымына, операциялық баптауларға және тағы басқаларға қандау қолжетімділікке рұқсат берілген?

6.7.4.2 Мәжбүрленген маршрутизация

Пайдаланушы терминалынан компьютердегі сервис аралығына дейінгі жол бақылануы қажет.

Аудит жүргізу жөніндегі басшылық:

Ұйымда мәжбүрленген маршрутизация саясаты қолданатын салаларда (қолжетімділікті бақылау саясатына сәйкестікке келтірілген жоғарыдан қараңыз) оның техникалық тұрғыда қалай жүзеге асырылғанын анықтаңыз және оны айналып өту әдістерінің жоқ екеніне көз жеткізіңіз. Желістік маршрутизацияның ыңғайлы ережелері жекелеген пайдаланушыларға кез-келген терминалға қосылуға мүмкіндік бере алады (әлсіз қорғалған аймақтар үшін бұл қауіпсіздік саясатына кереғар болуы мүмкін); хабарлар альтернативті желістік көпірлер арқылы бағыттала алады; телефон желілері мен басқа да ішкі қосылыстар сыйымдылық жетіспеген кезеңдерде және жөндеу жұмыстары жүргізілетін уақыттарда өзгертіле алады.

Ұйым желіс типологиясының нақты жоспарын ұсына алуы және басқарудың қандай құралдары мәжбүрлеп маршрутизациялауды жүзеге асыру үшін қолданғанын түсіндіре алуы қажет. Қолданған басқару құралдарының қажетті шектеулерді шын мәнінде жүзеге асыратынын тексеріңіз.

6.7.4.3 Сыртқы қосылыстар кезінде пайдаланушылардың сәйкестендірілуі және желіс тораптарының сәйкестендірілуі

Жойылған пайдаланушылардың сәйкестендірілуі жүзеге асырылуы қажет.

Жойылған компьютерлік жүйелерге қосылу сәйкестендірілуі қажет.

Аудит жүргізу жөніндегі басшылық:

Жойылған қосылыстар немесе сырттан кіруге жол беретін, қорғаныс жүйелерін пайдаланушы кез-келген ұйым аталмыш басқару құралының талаптарын толық көлемде орындауы қажет. Аудиторлар барлық порттар сәйкестендірілген және қатерлердің толық бағалануы жүргізілгенін тексеруі қажет.

Ең алдымен сәйкестендіру қандай деңгейде жүргізілетінін анықтау қажет – нақты қосымшалар деңгейінде ме, әлде желістік операциялық жүйе деңгейінде ме. Егер қосымшалар деңгейінде болса, мұндай сәйкестендіруді операциялық жүйе деңгейінде енушілердің жою-жоймауын түсінуге мүмкіндік беретін тестілер немесе баға беру шаралары жүргізілді ме? Қорғалатын ақпарат маңыздылығына шынайы қолданылған сәйкестендіру тетіктері балама ма? Басшылық болуы мүмкін қатерлер жөнінде толық мәлімденгеніне және басқарудың қажетті құралдарын қарастыруға тиісті назар аударғанына, ал басқарудың таңдалған құралдары дұрыс жүзеге асырылғанына және тұрақты түрде тексеріліп тұратынына көз жеткізіңіз.

Сәйкестендірудің көптеген тетіктері бар; таңдалған тетік (немесе тетіктер) қауіпсіздікті қамтамасыз ету жөніндегі талаптарға сәйкес екендігіне көз жеткізіңіз. Егер тікелей байланыстыратын қолжетімділік құралдары пайдаланылатын болса, олардың қалай жұмыс істейтінін анықтаңыз; жойылған тораптың сәйкестендірілуін тексеру үшін қолданыла алатын әдістердің бірі жауапты қоңырау шалу операциясы болып табылады, бірақ сәйкестендірудің сенімдірек әдістері қажет етілуі мүмкін, мысалы токендерді қолдану әдістері.

6.7.4.5 Желістерді сегментациялау

Желістерде ақпараттық жүйелер мен пайдаланушылар, ақпараттық сервистердің тобын бөлу үшін басқару құралдары жүзеге асырылуы тиіс.

Аудит жүргізу жөніндегі басшылық:

Домен неғұрлым үлкен болса, соғұрлым оның қорғанысын қамтамасыз ету қиынырақ болады. Бұл пікір басқа кез-келген құрылымдар сияқты, желістер үшін де шынайы болып табылады. Қорғалған желістерден өндірістік операциялардың кеңірек аспектілеріне – электронды поштаға, интернет-беттерге, басқа ұйымдардың желістеріне және т.б. қолжетімділікті қамтамасыз ету қажет болатыны айқын; осыған орай ерекше маңызды аймақтарды бөлу қажет.

Желістік ресурстарды бөлудің қажетті деңгейіне желісті сегменттерге физикалық бөлу арқылы немесе маршрутизация және желістік қосылыстарды басқару құралдарын жүзеге асыру жолымен, мысалы, көпірлер, маршрутизаторлар, желіс аралық экрандар және т.б. арқылы қол жеткізуге болады.

Аудиторлар қауіпсіздік домендерінің құрамын белгілеуі, олар қауіпсіздікті қамтамасыз ету жөніндегі талаптарға сәйкес келетінін, олар

желістік операциялар құрылымына қалай біріктірілгенін және анықталғанын тексеруі қажет. Сонымен қатар, қауіпсіздік домендерін пайдалану операциялық өнімділікті шектеу мүмкіндігін ескеру қажет, сондықтан осыған байланысты қорғалған аймақтардың қауіпсіздігін қамтамасыз ету тұрғысында ешқандай әшкереленуге жол берілмегеніне көз жеткізу керек.

6.7.4.6 Желістік қосылыстарды басқару және желістік маршрутизацияны басқару

Пайдаланушылардың ұжымдық түрде қолданылатын желістерге қосылу мүмкіндігі қолжетімділікті басқару саясатына сәйкес шектелуі тиіс.

Бірлесіп қолданатын желістерде компьютерлік жүйелердің қосылысы мен ақпараттық ағымдар өндірістік қосымшаларға қолжетімділікті басқару саясатын бұзбауы үшін маршрутизацияны бақылау құралдары қолданылуы қажет.

Аудит жүргізу жөніндегі басшылық:

Желістерді бірлесіп пайдаланған жағдайда пайдаланушылардың қосылыстарды орнату жөніндегі мүмкіндіктерін қолжетімділікті бақылау саясатына сәйкес шектеу қажеттілігі туындауы мүмкін. Егер пайдаланушылар мен сервистер физикалық қорғалған аймақтан тыс орналасқан және ашық қолжетімділігі бар көлік базасында желіс аралық қосылыстарды пайдаланатын болса, аудиторлар қосымшалар мен жүйелерге мұндай қолжетімділік түрі рұқсат етілгенін анықтауы қажет, егер рұқсат етілген болса, ішкі пайдаланушылар мен сервистердің қолжетімділігімен салыстырғанда оған қосымша шектеулер қойылатындығын тексеру қажет. Егер сервистерге қолжетімділіктің шектеулері қосымшалар деңгейінде артылса, онда локальды түрде қолданылатыннан ерекшеленетін, желістік басқару құралының пайдалану мүмкіндігі қандай, бұл қалайша жүзеге асырылған және саясатты жүзеге асыруға сәйкес келе ме?

Жойылған желістер арасындағы мәжбүрленген маршрутизация сыртқы тараптық жеткізімшілерге негізделуі мүмкін; егер мұндай жағдай орын алған болса, ұйымның маршрут бүтіндігі және қолжетімділігі қатысында қандай кепілдігі бар және оны пайдаланудың үздіксіздігі қалай қамтамасыз етіледі? Жөндеу жұмыстары және апаттар ұйымды басқа маршруттар пайдалануын мәжбүрлеген жағдайда не болады? Ашық қолжетімділікпен желіс арқылы өткен кезде белгілі маршрутты қамтамасыз ету мүмкін емес; бұл факт назарға алынды ма және қандай альтернативті көлік механизмдері қолданылады?

6.7.4.7 Желістік серверлерді қорғау

Ұйымда қолданылатын барлық серверлердің қауіпсіздік атрибуттарының нақты сипаттамасы ұсынылуы қажет.

Енгізу жөніндегі басшылық:

Сыртқы ұйымдарға ұсынылатын желістік сервистарға қосылу үшінші тұлғалар тарапынан рұқсатсыз кіру талпыныстары тұрғысында осалдыққа әкеледі, ал бұл құпиялықтың ашылуы мен бүтіндіктің жоғалуына әкеледі. Жабдықтардың сынуы немесе желістердегі ақаулықтардан соң жеткізімді сервистерінің қалыпты жұмыс жасауын қалпына келтіру қабілетін тексеріп, қолжетімділікке ерекше назар аудару қажет. Жеткізушінің қалпына келтіру жұмыстарын жүргізу уақытында қауіпсіздік стандарттарының орындалуын қамтамасыз етіңіз. Тәуекелдерді бағалау кезінде қауіпсіздікті қамтамасыз ету бойынша шаралардың нақтылығын ескеру қажет. Белгілі жағдайларда қорғаныстың әлсіз тұстарын өтеу үшін басқарудың қосымша құралдарын пайдалану қажет болуы мүмкін.

Аудит жүргізу жөніндегі басшылық:

Ұйым желістік қызметтердің сыртқы жеткізімшілеріне сүйенген жағдайда барлық сәйкес қауіпсіздік аспектілері жөнінде толық ақпаратқа ие болу қажет. Ұйымның мұндай ақпаратты алғанын, ол құжаттама түрінде бекітілгенін, қауіпсіздік белгілері жеткілікті және ұйым қажеттілігіне сай екеніне, алынған ақпарат қауіпсіздікті басқару құралдарында және операциялық процедураларда ескерілгенін және ол тұрақты түрде қарастырылып, тексеріліп тұратынын тексеріңіз. Аталған басқару құралдары құпиялық, бүтіндік және қолжетімділікті қамтамасыз етудің барлық аспектілерін қамтуы қажет екенін есте ұсаңыз.

6.7.5 Компьютерге қолжетімділікті басқару

Мақсаты: компьютерлерге рұқсатсыз кірудің алдын алу.

6.7.5.1 Терминалдардың автоматты түрде сәйкестендірілуі және терминалдан жүйеге кіру процедуралары

Желістің нақты тораптарына қосылысты сәйкестендіру үшін терминалдардың автоматты сәйкестендірілуі қолданылуы қажет.

Ақпараттық сервистерге кіру жүйеге кірудің сенімді процедурасының көмегімен жүзеге асырылуы қажет.

Аудит жүргізу жөніндегі басшылық:

Белгілі мекен-жайлар үшін және жүйелердің сәйкестендірілуіне арналған ықшам жабдықтарды қолдану кезінде терминалдың автоматтық сәйкестендірілуі қолданылуы мүмкін; кіру мүмкіндігіне тек табысты сәйкестендіруден соң ғана рұқсат етіле алады. Егер осыған ұқсас схема қолданылатын болса, сәйкестендіруді тексеру қалай орындалатынын, терминалда жаңылыс анықталған жағдайда және оны алмастыру қажет болса не болатынын анықтаңыз. Егер пайдаланушылардың қандай да бір түрде сәйкестендірілуі қажет болса, қорғаныстың тағы қандай құралдары қолданылады, терминал физикалық бекітілген бе немесе ол қорғалған аймақта орналасқан ба?

Жүйеде тіркелу процедуралары пайдаланушының аты мен паролын жай ғана дұрыс енгізуге қарағанда әлдеқайда кеңірек болуы мүмкін. Пайдаланушыдан тіркеу үшін әрекеттердің бірқатар тізбегін жүргізу талап етіле ме, ақпаратты дұрыс енгізбеген жағдайда не болады, кешеуілдеу кезеңдері бар ма, тіркеудің бірнеше сәтсіз талпыныстарынан соң жүйенің блокадалануы қарастырылған ба? егер қарастырылған болса, аталмыш жағдайдан шығудың тетіктері қандай?

Кейде қосымша тіркелу кезінде қорғаныстың жеткілікті деңгейін қамтамасыз ете алмайды – мысалы, сәтсіз талпыныстар саны шектелмеген жағдайда. Бұл жағдайда қосымша басқару құралдарының енгізілуін тексеру қажет (мысалы, терминалға кірудің физикалық шектелуі арқылы). Тәуекелдерді бағалауды жүргізу кезінде әрбір жүйе мен қосымша, қолжетімділік әдістері, сондай-ақ олардың баламалығын ескерілуі қажет - бұл осылай ма, тексеріп көріңіз.

6.7.5.2 Пайдаланушыларды сәйкестендіру және сәйкестендіру

Барлық пайдаланушыларға бірегей идентификаторлар (пайдаланушы идентификаторы) берілуі қажет, олар жекелеген тұлғалардың әрекетін бағдарлау мүмкіндігін қамтамасыз ету мақсатында тек қана осы пайдаланушылармен ғана қолданады. Пайдаланушының жарияланған аутентификациялық ақпаратын растау үшін сәйкестендірудің сәйкес әдісі таңдалуы қажет.

Аудит жүргізу жөніндегі басшылық:

«Пайдаланушы» термині жүйелік әкімгерлер, менеджерлер мен қосымша пайдаланушыларымен қоса, ақпаратты өңдеу жүйелері мен құралдарын қолданушы барлық тұлғаларды қамтуы қажет. Пайдаланушылардың бірегей сәйкестендірушілері қолданылатынын немесе сәйкестендірушілерді бірлесіп пайдалануға жол берілетінін тексеріңіз. Егер сәйкестендіруші бірнеше пайдаланушылармен қолданылатын болса, бұл не үшін қажетті, бақылау қалайша жүргізіледі және қандай рұқсаттар талап етілетінін анықтаңыз. Жүйелерге әкімшілік ету сияқты сындарлы қызметтер үшін тек аталмыш мақсатқа ғана арналған пайдаланушының сәйкестендірушісі болуы қажет, сонымен қатар қандай да бір оқиғаға бастамашы болған тұлға мен уақыттың тіркелуі қажет. Мұндай тіркеу журналдарын енгізу қандай жағдайлар үшін талап етілетінін, олар қанша уақыт аралығында сақталатынын, олардың түрлендірілуі мүмкін бе, қашан және қандай жағдайларда олар тексеріледі деген мәселелерді анықтаңыз. Егер нақты қосымшада мұндай ақпараттың бағамдалуы қарастырылмаған болса, басқарудың қандай құралдары қолданылатынын байқаңыз.

Ұйымда қолданылатын аутентификация процедуралары қорғалуы тиісті ақпарат, жүйелер және қосымшалар үшін қауіпсіздіктің жеткілікті деңгейін қамтамасыз ететіндігін анықтау қажет. Әдетте парольдерді пайдалану қатері жоғары салалар үшін қорғаныстың жеткіліксіз әдісі болып

саналады. Бұл жағдайда пайдаланушыларды сәйкестендіру және сәйкестендірудің тиісті процедураларын анықтау үшін қатерлерге баға беруді жүргізу қажет.

6.7.5.3 Парольдерді басқару жүйелері

Парольдерді басқару жүйелері сенімді парольдерді қамтамасыз етудің тиімді, интерактивті құралы болып табылуы қажет.

Аудит жүргізу жөніндегі басшылық:

Ұйымда парольдерді пайдалану жөніндегі жалпыға ортақ саясаты болуы қажет. Аса маңызды салаларға қойылатын кез-келген қосымша талаптар мүмкіндігінше, осы саясатқа сәйкестікке келтіріліп, оған қосымша ретінде рәсімделуі қажет. Аудиторлардың ерекше назар аударуы қажет аспектілердің қатарына төмендегілер кіреді:

– Парольдер ұзындығы мен құрамы;

– Парольдерді алмастыру жиілігі;

– әртүрлі пайдаланушылар мен қосымшалар үшін сәйкес келетін парольдерді пайдалану;

– парольдерді пайдалану және оларды сақтау кезіндегі қауіпсіздік;

– өздігінен парольді алмастыру.

Басқа жағдайлармен қатар, парольдерді алмастыру процессіне талдау жасау қажет: олар қайда және қалай тіркеледі, ескі парольдерді қолдануға шектеу қарастырылған ба, қосымша қабылданбас бұрын жаңа парольді растауды талап ете ме (мысалы, қайта енгізу жолымен). Қажет болған жағдайда пайдаланушылардың парольді ауыстыру процедурасын көрсетуін өтініңіз.

6.7.5.4 Жүйелік утилиталарды пайдалану

Жүйелік бағдарлама-утилиталарды пайдалану шектеліп, қатаң бақылануы қажет.

Аудит жүргізу жөніндегі басшылық:

Кейбір утилиталар қосымшалар үшін жабық жүйелер бөлігіне кіру мүмкіндігін береді және басқарудың жүйелік құралдарын айналып өтуді қамтамасыз ете алады. Аудиторлар ең алдымен ұйымның орнатылған утилиталардың жалпы бақылауын қамтамасыз ететінін анықтауы қажет, утилиталар тізімі белгілі және олардың қолданысқа рұқсат етілгенін және олармен жұмыс істеу кезінде қолжетімділікті шектеу мен сәйкес қадағалау қолданылатынын тексеруі қажет. Жекелеген жүйелерде қосымша немесе түрлендірілген утилиталар орнатылмағанын тексеріңіз.

Қауіпсіздік жүйесі жеткіліксіз реттелетін ұйымдарда қолданылуы ақпараттың құпиялылығына ғана емес, оның бүтіндігі мен қолжетімділігіне нұқсан келтіруі мүмкін шартты-тегін утилиталар орнатылуы мүмкін. Сонымен қатар, жүйелер жадында жойылуы тиіс ұмыт қалдырылған резидентті утилиталардың қалмауын тексеріңіз. Және соңында сәйкес рұқсат

алған тұлғалардан басқа ешкім жүйелік утилиталарға кіре алмайтынын және оларды қолдана алмайтынын тексеріңіз.

6.7.5.5 Пайдаланушылар қорғанысына арналған мәжбүрлеу туралы ескертуші дабыл белгісі

Мәжбүрлеу объектісі болуы мүмкін пайдаланушылар үшін мәжбүрлеу туралы ескертуші дабыл сигналын пайдалану мүмкіндігі ұсынылуы мүмкін.

Аудит жүргізу жөніндегі басшылық:

Ұйым мәжбүрлеу туралы ескертуші дабыл сигналын пайдалану қажеттігін сәйкестендірілген тұстарда, аудитор ең алдымен, барлық қажетті талаптардың орындалғанына назар аударуы қажет: мысалы, барлық мүмкін нүктелер қамтылды ма, қажетті жерлерді дабыл сигналы беріле ме, сигналды шегеруге бола ма?

Сигналдың активациясы қарапайым болуы қажет, бірақ оның қарапайымдылығы жалған белгілер беретіндей қарапайым болмауы қажет. Дабыл сигналы физикалық түрде активациялануы қажет, мысалы, батырманы басу немесе қосымшамен жұмыс кезінде арнауы кодты енгізу арқылы. Кейбір дабыл сигналдары үшін, қызметкерлерді босқа әбігерге түсірмеу мақсатында активацияның байқалмайтын әдісі қарастырылуы қажет.

Әрекеттері мен міндеттері ерекше белгіленетін, қатер сигналдарына әрекет ету процедураларын қарастырыңыз. Дабылға реакция кезіндегі бастапқы әрекеттер түсіну үшін қарапайым болуы қажет және қажет жағдайда дереу орындалуы қажет; мұнда аудитор сәйкес қызметкерлердің нұсқаманы оқымай-ақ, тым болмаса әрекет ету процедураларымен қарастырылған бастапқы қадамдарда не істеуі қажет екенін білетінін тексергені жөн.

6.7.5.6 Терминалды уақыт бойынша блокадалау және қосылу уақытын шектеу

Тіркелмеген пайдаланушылардың жоғары қатер аймақтарында орналасқан немесе жоғары қатерлі жүйелерге қызмет көрсетуші, әрекетсіз терминалдарға қолжетімділігін болдырмау үшін белгіленген әрекетсіздік кезеңі өткен соң бұл терминалдардың сөндірілуі қажет.

Жоғары қатерлі қосымшаларды үстеме қорғау үшін қосылу уақытына шектеулер қолдануы қажет.

Аудит жүргізу жөніндегі басшылық:

Белгілі уақыт өткен соң белгілі әрекетсіз терминалдардың сөндірілу мүмкіндігі қауіпсіздігі жеткіліксіз деңгейде тексерілген қызметкерлер қолжетімділігі немесе ашық қолжетімділік мүмкін болған кез-келген жағдайларда қарастырылуы қажет. Сәйкес шаралар қайда анықталғанын және операциялық талаптар, осалдық, қолжетімділік деңгейі тұрғысынан қарағанда таңдалған кезеңдер жеткілікті екенін байқаңыз. Жұмыс

істеу/әрекетсіздік анықтамасы неге негізделгенін, қосымшаның белгілі қолданысына немесе қарапайым тінтуірдің қозғалысына негізделгенін біліңіз. Әрекетсіздік кезеңі бойынша сөндірілуі кезектілікпен барлық жоғары қатер тұстарында қолданылатынын тексеріңіз – ашық қолжетімділікті кейбір кеңселік бөлмелерде мұндай қорғаныс әдісін талап ететін бірнеше терминалдар болуы мүмкін – және аталмыш схема барлық жерде қызмет жасауға қабілетті екенін тексеріңіз. Сөндірілуі әрекетсіздік кезеңі бойынша Windows экран қорғағышы сияқты, операциялық жүйе қызметтеріне негізделген жерлерде қажетті қызметтің сөндірілмегенін, сонымен қатар парольді қолдану қабылданған саясатқа сәйкестікте жүргізілетініне көз жеткізіңіз.

Кейбір қосымшаларда әрекетсіздік кезеңі бойынша блокадалаумен қатар қосылу уақыты бойынша шектеулер қолдануы мүмкін. Қосылыс бойынша шектеулер қатердің жоғары деңгейіне жататын қосымшаларда қолдануы қажет. Қайтадан аталмыш әдіс қайда қолданылатынын анықтап, оның қолданысы талаптарға сәйкес келетінін тексеріп, мысалы қандай да бір транзакцияны аяқталмаған күйінде қалдырып, таймерларды айналып өтуге болмайтынын тексеру қажет.

6.7.6 Қосымшаларға кіру мүмкіндігін басқару

Мақсаты: Ақпараттық жүйелерде сақталатын ақпаратқа рұқсатсыз кірудің алдын алу.

6.7.6.1 Ақпаратқа қолжетімділікті шектеу

Ақпараттар мен қолданбалы жүйелердің қызметтерін пайдалану мүмкіндігі қолжетімділікті басқару саясатына сәйкес шектелуі қажет.

Аудит жүргізу жөніндегі басшылық:

Аудиторлар ең алдымен жекелеген қосымшалармен ұсынылатын ақпаратқа қолжетімділік өндірістік талаптарға сәйкес келетініне және қолжетімділікті басқару саясатына сәйкес жүргізілетініне көз жеткізуі қажет. Мысалы, бір деректер базасына қолжетімділік әртүрлі қосымшалардан жүзеге асырылуы мүмкін; бір қосымша көмегімен, басқа қосымша үшін рұқсат етілмеген құпия ақпаратқа қолжетімділік алуға бола ма?

Көптеген жағдайларда пайдаланушылар қолданысы олар үшін рұқсат етілмеген қосымшалар қызметтері немесе ақпарат туралы білуі тиіс; сәйкесінше қауіпсіздік мақсаттарында рұқсат берілмеген меню тармақтарын көрсетпеуге тырысу қажет. Дәл осы жағдай нақты қосымшалар бойынша пайдаланушылардың басшылығына да қатысты. Сүйемелдеуші утилиталар сияқты сирек қолданылатын қосымша компоненттеріне ерекше назар аударыңыз: олармен жұмыс бойынша жеткілікті бақылау жүзеге асырыла ма?

Сонымен қатар, қолжетімді ақпаратқа қатысты қандай әрекеттер жасалып жатқанын анықтау қажет: пайдаланушыларға ақпаратты оқуға,

жазуға рұқсат етілген бе, мұның қажеттілігі бар ма, ақпаратты шығаруға шектеулер қойыла ма? Желістік жүйелердегі басылым оператордан ажыратылған бірлескен қолжетімділік құрылғыларында орындала алады - бұл жағдайда бақылау қалайша жүзеге асырылады? Ақпаратты қорғау кезінде қауіпсіздікті жіктеу жүйесіне сәйкестікті қамтамасыз ету қажет.

6.7.6.2 Осал жүйелерді оқшаулау

Осал жүйелер ерекшеленген (оқшауланған) санау ортасына ие болуы қажет.

Аудит жүргізу жөніндегі басшылық:

Осалдық деңгейі жоғары ақпаратты пайдалану сөз болатын жерде қандай да бір деңгейде оқшаулауды жүзеге асыру қажеттілігі туындауы мүмкін. Мұндай салалар осы орайда қауіпсіздік, қолжетімділік және операциялық мәселелерді назарға алатын ұйыммен сәйкестендірілуі қажет. Жүйе соншалықты жоғары қауіпсіздік талаптарын қоюы мүмкін, сондықтан оның оқшаулану немесе балама нұсқама ретінде, бөлінген қорғалушы порт арқылы басқа жүйелермен байланысты жүргізу қажет болуы мүмкін.

Қарапайым процедуралар мен анықтамалардан басқа, мұндай жүйелердің қатерлерге баға беру аясында сәйкестендірілгеніне, ал оларды оқшаулау қажеттігі жеткілікті түрде дәлелденгеніне көз жеткізіңіз – қолжетімділіктің қатаң бақылануы (оқшаулау жағдайында сияқты) жүйені орындау жөніндегі өндірістік талаптармен қайшылыққа келуі мүмкін; бұл екі мәселе арасында ортақ оңтайлы шешім қабылданғанын тексеріңіз. Егер жеке жүйені бөлу қажет болса, жаңылыстан соң жұмыс қабілетін қалпына келтіру бойынша қандай шаралар қарастырылғанын анықтаңыз, деректерді енгізу немесе ақпарат таратушыларынан бағдарламаны жүктеуге қандай шектеулер қойылады, қандай резервтік көшірмелер құрылады.

6.7.7 Қолжетімділік мониторингі

Мақсаты: Заңсыз әрекеттерді анықтау.

6.7.7.1 Оқиғаларды тіркеу

Барлық шектен тыс оқиғалар және қауіпсіздіктің бұзылуына байланысты басқа да оқиғалар бақылау журналында тіркелуі қажет. Мұндай журналдардағы жазбалар қолжетімділікті басқару саясатын орындауды тексеру және зерттеу үшін кейін қолдану мақсатында белгілі уақыт аралығында сақталуы тиіс.

Аудит жүргізу жөніндегі басшылық:

Ақпараттың өңделуі жүзеге асырылатын барлық жүйелер үшін пайдаланушыға тәуелсіз және оның қолы жетпейтін қандай да бір формадағы журнал жүргізілуі қажет. Аудиторлар мұндай әдіс қауіпсіздік жөніндегі талаптарға сай келетін саланы анықтап, оның ұйымда жүзеге асырылуын зерттегені жөн. Жазбаларды сақтау саясатына сәйкес немесе

куәліктерді жинау мақсатында белгілі уақыт аралығында сақталуға тиісті барлық жазбалар тиісті түрде мұрағатқа өткізілгеніне көз жеткізіңіз. Журналдарда нақты не тіркеледі? Кем дегенде онда оқиға туралы, оқиға жөнінде хабарлаған тұлға, орындалған шаралар (бұл қолданылатын жерде), күні мен уақыты туралы ақпарат мазмұндалуы қажет. Қосымша транзакция кодтары мен терминал сәйкестендіргіштерінің тіркелуі қажет болуы мүмкін. Оқиға деп не саналатынын анықтаңыз және барлық ерекшеліктер ескерілгеніне көз жеткізіңіз. Тіркелген ақпаратты қаншалықты ұзақ, қандай түрде және қандай қорғаныс құралдарын пайдалана отырып сақтау қажеттігін анықтаңыз; талаптардың орындалуын тексеріңіз. Оқиғалар мысалы ретінде жүйелік администраторлармен өзгеріс енгізуді, сондай-ақ жүйеге енудің сәтсіз талпыныстарды, сондай-ақ деректерді ашуды жүзеге асыруды келтіруге болады.

6.7.7.2 Жүйені пайдалану мониторингі

Ақпаратты өңдеу құралдарын пайдалану мониторингі процедуралары анықталып, аталмыш мониторингтердің нәтижелері үнемі сарапталып тұруы қажет.

Аудит жүргізу жөніндегі басшылық:

Мониторинг қауіпсіздік жағдайларының журналында қарастырылмаған әрекеттер белгілерінің болуына тексеруді қамтиды. Қатерлерге берілген баға қайда және қандай мониторинг жүргізу қажеттігін көрсетуі қажет. Мысалдар ретінде төмендегілерді атауға болады:

– кірудің сәтсіз талпыныстары;

– деректердің ерекше мәндері;

– қорғалған деректерге өзгертулер енгізу талпыныстары;

– белгілі деректерді шамадан тыс көп пайдалану;

– пайдаланушының сирек қолданылатын немесе артық идентификаторымен кіру.

Жоғарыда айтылғандай жазбалармен жұмыс қалай жүргізіліп жатқанын тексеру және олардың түрленуі және өшірілуі мүмкін емес екеніне көз жеткізу қажет.

Аудиторлар нәтижелердің дұрыстығын кепілдеу мақсатында әрекеттердің анализі бойынша және талданатын әрекеттердің өзі бойынша қызметтер тұрғысында міндеттердің бөлінісін қамтамасыз ету үшін ұйымда қандай шаралар жасалғанын қарастыруы қажет.

Сонымен қатар, тіркеу журналдары қаншалықты жиі зерттелетінін тексеруі қажет – қауіпсіздік қатысында тәуекел деңгейі неғұрлым жоғары болса, соғұрлым журналды жиірек қарастыру қажет. Мұндай тексеріс журналдар деректерінің анализі процессінде өнімділік және тиісті тиімділікті қамтамасыз ету үшін жүргізілуі қажет.

Оқиғаларды тіркеу процессімен немесе жүйемен басқарылатын журналдар көбіне үлкен көлемді болуы мүмкін. Сәйкесінше, бұл қауіпсіздік инциденттері жөніндегі аудит үшін маңызды ақпарат одан маңызы төмен басқа ақпараттар арасында жоғалуына әкелуі мүмкін. Осылайша, барлық қажетті инциденттер мен әрекеттердің іріктелуін қамтамасыз етуші сүзу ережесін қолдана отырып, аудит журналының сүзу құралдарын пайдалану қажет. Аудитор ұйым қызметкерлерінен мұндай құралдарының болуы және пайдаланылуы жөнінде сұрастыруы және оқиғаларды анықтау мен оларға әрекет ету үшін бұл құралдардың қолданылуын анықтауы қажет.

6.7.7.3 Жүйелік сағаттарды үйлестіру

Бақылау журналдарының нақтылығын қамтамасыз ету үшін компьютерлердің жүйелік сағаттары үйлестірілуі қажет.

Аудит жүргізу жөніндегі басшылық:

Барлық жүйелерде уақыт үйлестірілмейінше оқиғаларды тіркеу нақты болмауы мүмкін, ал бұл оның жалғандығына әкелуі мүмкін. Ұйым уақыт санағы үшін базаны орнатуға міндетті; көпшілік жағдайларда бұл жергілікті уақытқа көшіру болуы мүмкін, бірақ халықаралық ұйымдар үшін басқа базаны пайдалану қолайлы болуы мүмкін, мысалы Гринвич бойынша (GMT) уақытқа көшу. Сонымен қатар, қажет болған жағдайда уақытты түзетуге мүмкіндік беруші жүйелі сағаттардың мониторинг құралы қарастырылуы қажет.

Жазғы уақыттан қысқы уақытқа көшу қалай жүргізілетінін анықтаңыз. Портативті жүйелер желісіне қосылу кезінде қандай да бір қосымша тексерістер жүргізіле ме? Оқиғаларды тіркеу жүйелік сағаттардың дәлдігіне сүйенеді, уақытты ауыстыру жазбалардың жалғандығы үшін қолданылуы мүмкін; жүйелік сағаттарды өзгерту мүмкіндігі шектеулерінің болуын тексеріңіз. Сонымен қатар оқиғаларды қолмен тіркеу қажеттілігі кезінде, мысалы жүктерді жеткізу және инциденттер туралы мәлімдеу кезінде қолданылуы мүмкін қабырға сағаттары туралы есте ұстаңыз.

6.7.8 Мобильді есептеулер мен қашықтан жұмыс

Мақсаты: мобильді есептеулер мен қашықтан жұмыс құралдарын пайдалану кезінде ақпараттар қауіпсіздігін қамтамасыз ету.

6.7.8.1 Мобильді есептеулер

Мобильді есептеу құралдарымен, әсіресе қызмет етудің қорғалмаған ортасында жұмыс істеуге байланысты қатерлерден қорғанысқа арналған сәйкес басқару құралдары таңдалып, формальды саясат құрылуы қажет.

Аудит жүргізу жөніндегі басшылық:

Ұйым кез-келген мобильді есептеу құрылғыларын пайдалану фактілерін сәйкестендіруі қажет; мұнда мобильді телефондар, лэптоп, ноутбуктар мен қалталы компьютерлерді ұйым аймағынан тысқары

(мысалы, үйде, тапсырысшы аумағында, қонақ үйлерде және мәжіліс ұйымдастырылатын жерлерде) қолдану, сондай-ақ осындай құрылғыларды пайдалана отырып, ұйымда ақпараттың өңдеудің сыртқы құралдарына кез-келген алынбалы қосылыстарды пайдалану кіреді. Мұндай құрылғыларды және жабдықтарды пайдалану кеңінен тарағандықтан, ал мобильді есептеулер ұйымнан тысқары жүргізілетіндіктен, мұндай қолданыстың тікелей аудитін жүргізу қиын.

Осыған байланысты, мұндай мобильді құралдарды қауіпсіз пайдалануды қамтамасыз ету үшін ұйымда жүзеге асырылған процедуралар мен ережелерді, басқару құралдарын мұқият талдау өте маңызды болып табылады. Бұл атап айтқанда, мұндай құрылғылардың жеке қорғанысы үшін қолданылатын басқару құралдарын қамтиды.

Сонымен қатар, жоғарыда аталған барлық басқару құралдары дұрыс жүзеге асырылғанын тексеру қажет. Басқару құралдарын тексеру кезінде мобильді компьютерлерге қолданыста вирустардан қорғау және парольдерді қорғау мәселелері сәйкес саясатта қалай белгіленгенін анықтау қажет. Алынып тасталған қолжетімділікті қорғану үшін жеткілікті басқару құралдарының болуына, ал бұл қажет етілген жерлерде криптографиялық қорғаныс құралдарының қолданылатынына көз жеткізіңіз.

6.7.8.2 Қашықтан жұмыс

Қашықтан жұмысты шешу және бақылауға арналған саясаттар, процедуралар және стандарттар жасақталуы қажет.

Аудит жүргізу жөніндегі басшылық:

Дистанциялық жұмыс тек өшірілген қосылыстың қауіпсіздігін қамтамасыз ету және қолжетімділікті бақылауды басқару, жеке қорғаныс құралдарымен қоса, жеткілікті басқару құралдары болған жағдайда және жүзеге асырылған кезінде ғана рұқсат етілуі қажет. Үйде қолданылатын жабдық ресурстардың мүліктік тізіміне енгізілуі қажет. Сонымен қатар, жұмыс процессінде пайдаланылатын, жұмыс орнынан алынып, үйдегі жұмыс орнына өткізілетін ақпаратты анықтау және бақылау механизмдері болуы қажет.

Компьютерлік ойындар, Интернетке кіру мүмкіндігі және т.б. сияқты бөгде қызметтер үшін жабдықтарды пайдаланудың белгілі саясаты болуы қажет, себебі кез-келген қызмет маңызды және құпия ақпаратпен бірге қолданылған жағдайда күрделі проблемаларға әкелуі мүмкін.

6.8 Ақпараттық жүйелерді жасақтау және сүйемелдеу

6.8.1 Жүйе қауіпсіздігіне қойылатын талаптар

Мақсаты: Ақпараттық жүйелерде қорғаныс құралдарының құрылымын қамтамасыз ету.

6.8.1.1 Қауіпсіздік талдауы және оған қойылатын талаптар

Жаңа жүйелерге арналған бизнес-талаптар немесе сәйкес жүйелерге арналған жетілдірулер басқару құралдары жөніндегі талаптарды айқындайды.

Аудит жүргізу жөніндегі басшылық

Ұйымдар қауіпсіздік жөніндегі талаптардың бағдарлама-қосымшалар, жаңа жүйелерді жасақтау, жүйелерді жетілдіру және жаңарту үшін анықталған және есепке қабылданғанын көрсете алуы қажет. Іс жүзінде бұл екі санатпен ұсынылған, мұнда белгіленген қосымшалардың БҚ нақты ұйым үшін немесе ұйымның өзімен жасақталады немесе дайын коммерциялық БҚ (COTS) қорғалған ортада пайдалану үшін сатып алынады. (COTS БҚ толық бағдарлама-қосымшаны немесе оның құрылымдық компонентін құрай алатынын ескерте кету қажет.)

Талаптардың бастапқы талдауы қауіпсіздік мәселелерін сәйкестендіру және оларды жаңа жүйелер үшін және/немесе бағалау туралы есептерге арналған қосымшаларға пайдаланушылық талаптары бар құжаттарда оларды қарастыру үшін қажет. Аталмыш процедура аяқталған соң аудитор аталмыш талаптардың жүйені жасақтау және енгізу кезінде қалай бақыланып, тексерілетінін қарауы қажет. Кез келген проблемалар талданып, менеджменттің сәйкес деңгейінде қарастырылып, қанағаттандырарлықтай шешілуі қажет.

6.8.2 Қолданбалы жүйелердегі қауіпсіздік

Мақсаты: Қолданбалы жүйелерде пайдаланушылардың деректерінің жоғалуын, түрлендірілуін және рұқсатсыз пайдаланылуын болдырмау.

6.8.2.1 Кіріс деректерінің шынайылығын тексеру және деректердің сыртқы өңделуінің шынайылығын тексеру

Жүйе-қосымшаларға деректерді енгізу дұрыс және тиісті жолмен жүргізілгенін куәландыру үшін, ол сәйкес түрде расталады.

Растаушы тексерістер деректердің өңделуі кезіндегі кез-келген жаңылысты анықтау үшін жүйелерге енгізіледі.

Аудит жүргізу жөніндегі басшылық

Қосымшаның бағдарламалары деректерді енгізу, сондай-ақ деректерді өңдеу кезінде деректердің бүтіндігін тексерудің тиісті деңгейін ұсынуы қажет. Деректер қолмен енгізілгенде, аудитор белгіленген аяға сәйкес келмейтін айқын бұрыс мәндер, дұрыс емес мәндер мен толық емес деректердің қабылданбайтынына көз жеткізуі қажет. Егер деректер қағаз формасында ұсынылатын болса (операторлардың соңынан енгізуі үшін), бұл деректер үшін қандай растама берілетінін байқау қажет – аталмыш құжаттар оған уәкілеттігі жоқ қызметкерлермен бағалана ала ма? Айқын өзгертулер болған жағдайда, олар тексеріліп, бекітіле ме? Деректер үлдір немесе диск сияқты басқа арналар арқылы енгізілсе, олар тиісті жолмен белгіленгенін

және қолданысына дейін тозбайтынына көз жеткізуі қажет. Деректер жүйеге енгізілген соң, жүйе қателіктері немесе әдейі өзгертулер салдарынан қателіктер пайда болуы мүмкін. Жасақталу жөніндегі құжаттамада бүтіндікке тағы қандай тексерістер жүргізуге болатынын анықтау қажет және олар орындау мүмкіндігіне және талаптарға сәйкестігіне көз жеткізу қажет. Жүйенің жасақтамасы деректердің жарамсыз болып қалуы қатерін төмендетіп, деректердің кез-келген зақымдалуын анықтау үшін тексерістер орындалатынын кепілдеу қажет.

6.8.2.2 Хабарларды сәйкестендіру

Хабарлар мазмұнының бүтіндігін қорғау жөніндегі қауіпсіздік талаптарының қосымшасы үшін хабарлардың сәйкестендірілуі қолданылады.

Аудит жүргізу жөніндегі басшылық

Аудиторлар ұйымда хабарлардың сәйкестендірілуі қолданылатындығын сұрастыруы қажет, егер қолданылатын болса, оның тетіктері дұрыс қолданылатынын тексеру қажет. Ұйым қатерлерді анықтау үшін тәуекелдердің бағалануын беруді жүргізуі қажет және олардың мазмұнының бүтіндігін сақтау үшін хабарлар сәйкестендірілуі қажет болуын анықтауы қажет, егер мұндай сәйкестендірілуі қажет етілетін болса, оның енгізудің ең оңтайлы нысаны қандай. Пайдаланбаған әдістерді тексеру кезінде, аудитор қатерлерді бағалау нәтижелерін есепке алуы қажет.

Хабарлардың сәйкестендірілуін пайдалану қажет болатын жағдайлардың мысалдары:

– Электронды сауда немесе басқа электронды қызмет саласында қандай да бір белсенділік ретінде құжаттармен және хабарлармен алмасу;

– Электронды хабарлар және/немесе файлдармен алмасу; және

– Хабар мазмұнының бүтіндігі өте қажет және өмірлік маңызы бар болып табылатын басқа кез-келген қосымша.

6.8.2.3 Сыртқы жіберілетін деректер шынайылығын тексеру

Сақталатын ақпараттың өңделуі дұрыс және жағдайларға сәйкес болып табылатынына көз жеткізу үшін, жүйе-қосымшадан сыртқа шығарылатын деректер тексерілген болуы қажет.

Аудит жүргізу жөніндегі басшылық

Жүйе-қосымша шығарылатын нақты деректерді ұсынуы қажет және ұйым шығарылатын деректердің нақтылығын тексеру және дұрыс емес немесе толық емес шығарылған деректерді алуға реакция беру тетігіне ие болуы қажет. Аудиторлар қызметкерлердің аталмыш процедуралармен таныс екеніне көз жеткізу үшін, мүмкін ағат тұстарын іздеу немесе аталмыш процедураларды айналып өту мүмкіндіктерін анықтау үшін, шығыс деректерінің мұндай тексерістерге қатысуы қажет. Олар сонымен қоса, аталмыш процедуралар үшін жауапты тұлғалар анықталғанын және өз міндеттерін білетіндігін тексеруі қажет.

Шығыс деректерін растау тестілеріне тексеру аяқталған соң, олардың нәтижелері заңсыз жолмен өзгертіле алмайтынына көз жеткізу қажет.

6.8.3 Бақылаудың криптографиялық құралдары

Мақсаты: Ақпараттың құпиялығын, ақиқаттылығын немесе бүтіндігін сақтауды қамтамасы ету.

6.8.3.1 Бақылаудың криптографиялық құралдарын пайдалану саясаты

Ақпаратты қорғау үшін криптографиялық басқару әдістерін пайдалану саясатын жасақтау қажет.

Аудит жүргізу жөніндегі басшылық

Басқарудың криптографиялық элементтерін қауіпсіз және тиімді қолданудың маңызды аспектісі аталмыш басқару элементтерін күнделікті қолдау саясатын қолдану және пайдалану тетіктері туралы дұрыс шешімдер қабылданғанын куәландыру болып табылады. Аталмыш саясат басқарудың криптографиялық элементтері қолданылуы қажет жағдайлар мен ақпаратты, басқарудың криптографиялық элементтерін қолдануға қатысты менеджментпен қолданылатын негізгі тәсіл, рольдер мен міндеттерді қамтуы қажет.

Егер ұйым басқарудың криптографиялық элементтерін қолданатын болса, аудиторлар басқарудың криптографиялық элементтерін пайдалану саясаты жасақталғанына, таратылғанына және қызметкерлердің барлығы онымен таныс және оны орындайтынына көз жеткізуі қажет. Олар қабылданған шешімдер тәуекелдердің бағалануының нәтижелерімен қолданылатынын және қолданылатын басқару элементтері аталмыш саясатқа сәйкестігін анықтауы қажет.

Басқарудың криптографиялық элементтерінің күші өзгерілерді және қолданылатын алгоритмдер, негізгі мөлшерлер және параметрлермен сәйкестендіріледі. Басқарудың криптографиялық элементтері қолданылатын қосымша және ортаны ескеру қажет. Кейбір қосымшалардың ортасы одан да күштірек басқарудың криптографиялық элементтерін талап етуі мүмкін.

Осылайша, ұйым қолданатын әдістер оған сай келе ме деген сұраққа жауап беру үшін, аудиторлар криптографиялық техникалар мен механизмдер, негізгі менеджмент және олардың ресурстарға қолданылатыны туралы кем дегенде жалпы мағлұматқа ие болуы қажет.

6.8.3.2 Шифрлау, Сандық қолтаңбалар және үздіксіздік сервисі

Осал және сындарлы ақпараттың құпиялылығын сақтау үшін шифрлау пайдалануы қажет.

Электронды ақпараттың ақиқаттылығын және бүтіндігін қорғау үшін сандық қолтаңбалар қолдануы қажет.

Қандай да бір оқиғалар немесе әрекеттердің болу-болмауы туралы даулы мәселелерді шешу үшін үздіксіздікті қамтамасыз ету сервистері қолданылуы қажет.

Аудит жүргізу жөніндегі басшылық

Аудиторлар сонымен қатар, шифрлау, сандық қолтаңбалар және/немесе үздіксіздікті қамтамасыз ету сервистері қолданылатын шарттарды тексеріп, олардың белгілі бизнес талаптар саясатына және қауіпсіздік талаптарына сәйкестігін анықтауы қажет.

Сонымен қатар, олар келесі жағдайларды тексеруі қажет:

– Шифрлау, сандық қолтаңба немесе үздіксіздікті қамтамасыз ету сервистерінің қолданылу немесе қолданылмауы туралы шешім қабылданғанда тәуекелдердің бағалануы пайдаланды ма және олардың қорғанысы бойынша нақты талаптарды анықтаңыз;

– Сәйкес алгоритмдер мен кілт ұзындығы таңдалды және олар тәуекелдердің бағалануы нәтижелері және қорғаныс жөніндегі белгілі талаптармен сәйкестендірілген;

– Криптографиялық тетіктердің қосымшасын пайдалануға қатысты процедуралар және экспорт пен импорт ережелерімен қоса, кез-келген қолданыстағы заңнама анықталған және орындалады;

– Менеджмент кілттерінің барлық тиісті жүйелері кілттерді қорғау мақсатында және оларды қауіпсіз сақтау және пайдаланудың кепілі ретінде қолданылады.

Аудиторлар қызметкерлердің басқарудың криптографиялық элементтері саясаты туралы білетінін, және мысалы, криптографиялық бақылаудың қолданылуын қадағалай отырып, оларды қашан пайдалану қажеттігін білуін сұрап анықтауы қажет.

6.8.3.3 Кілттерді басқару

Криптографиялық әдістерді қолдау үшін келісілген стандарттар, процедуралар мен әдістердің жиынтығына негізделген кілттерді басқару жүйесі қолданылуы қажет.

Аудит жүргізу жөніндегі басшылық

Кілттерді басқару басқарудың криптографиялық элементтерін қауіпсіз қолданудың қажетті шарты болып табылады; криптография кілттерді басқарудың дайын қорғалған жүйесіз қолданбауы қажет. Аудиторлар ұйымның келесі қорғанысын қамтамасыз етуі үшін қажетті басқару құралдарын қолданғанын тексеруі қажет:

– Ашылу, өзгерту немесе бұзудан қорғаудың құпия және жекеше кілттері;

– Қоғамдық кілттер және рұқсатсыз өзгерту мен бұзудан қоғамдық кілттердің сертификаттары; егер ұйым өзінің қоғамдық кілттерін басқару үшін (жеке немесе қоғамдық) сертификациялық басшылардың қызметін

пайдаланатын болса, аталмыш басшылардың балама қорғалған, сенімді және басқарылатынына көз жеткізу қажет.

Криптографиялық кілттердің қорғанысы логикалық және физикалық қорғаныстыүйлестіруі қажет. Аудиторлар криптографиялық кілттерді қорғау үшін қолданылатын, қолжетімділікті басқарудың физиологиялық және логикалық аспаптарын тексеруі қажет. Егер кілтті депонирлеу немесе қалпына келтіру механизмі немесе процессі криптографиялық кілттерге қолданылатын болса, қызметкерлердің бұл туралы білетініне және кілтті депонирлеуді айналып өту мүмкін емес екеніне көз жеткізу қажет.

6.8.4 Жүйелік файлдардың қауіпсіздігі

Мақсаты: ақпараттық жүйелердің жасақталу жобасының сенімді жүзеге асырылуын және оның қолдауын қамтамасыз ету.

6.8.4.1 Жұмыс істейтін бағдарламалық құралды қадағалау

Жұмыс жүйелерінде бағдарламалық құралды орнатуды қадағалау үшін процедуралар қарастырылуы қажет.

Аудит жүргізу жөніндегі басшылық

Аудиторлар ҰЖ БҚ енгізуге қолданылатын басқару элементтерін тексеруі қажет – жүйелік кодтың күйі қандай, код көзі қосылған ба, жаңа нұсқалар қалай енгізіледі, жүйелік файлдар мен кітапханалар қалай қорғалады, өзгерістер туралы қандай жазбалар жасалады? Қолдауды жасаушылар мен қызметкерлер ҰЖ тестіленбеген немесе рұқсат етілмеген кодтарды енгізу қауіптері туралы білуі қажет, олардың бұл жағдайды ұғынатынын тексеру қажет.

Содан соң оның енгізілуіне назар аудару қажет - бастапқы мәтін мен объектінің кодтарына қандай қорғаныс қолданылады, жаңа немесе өзгертілген кілтті енгізбес бұрын тестілеудің қандай кезеңдері аяқталған болуы қажет, регрессивті тестілеу дұрыс па, кілттің ескі нұсқалары қайтадан инсталляцияланууы мүмкін бе, өзгертулер енгізілмес бұрын деректердің толық көшірмесі сақтала ма?

Операциялық кодта өзгертулер жазбаларын қарастыру қажет, олар толық па, жеткілікті түрде сипатталған ба және тиісті рұқсаты бар ма? Маңызды операциялардың кешені жаңа және өзгертілген кодты енгізу үшін егжей-тегжейлі мұқият қарастырылған жоспарды талап етуі мүмкін, мысалдар келтіріңіз.

6.8.4.2 Жүйелік тестілік деректерді қорғау

Тестілік деректердің қорғанысы және бақылануы қамтамасыз етілуі қажет.

Аудит жүргізу жөніндегі басшылық

Аудиторлар тестілеу үшін қолданылатын деректер тиісті жолмен бақыланатынына көз жеткізуі қажет. Тестілер жаңғыртыла алуы қажет,

осылайша қолданылған деректер нақты айқындалған және қайта тестілеу үшін қолжетімді болуы қажет. Осы деректердің тестілеу үшін қолдануы мақұлданбайды, ал қолдана қалған жағдайда кез-келген жеке немесе маңызды ақпаратты шектеу үшін өзгертілуі қажет. Бұл үнемі мүмкін бола бермейді және мұны әрқашан кепілдеу мүмкін емес, сондықтан олардың немесе тестілердің кез-келген нәтижелері, файлдар мен жазылған нәтижелермен бірге қалайша қорғалғанын тексеру қажет.

Тестілеу үшін аталмыш деректерді қолдану әрбір жағдайда тиісті түрде рұқсат етілгенін тексерген жөн. Сонымен қатар, қолжетімділікті бақылау және тестілеу кезінде деректер базасына енгізілген кез-келген деректерді толық жою үшін дайын әдістің болуын тексеру қажет. Тестілеу бойынша жүйе-қосымшаларға қолжетімділік ҰЖ қолжетімділік сияқты қатаң бақылануы қажет.

6.8.4.3 Бағдарламалардың бастапқы мәтіндерінің кітапханаларға енгізілуін қадағалау

Бағдарламалардың бастапқы мәтіндерінің кітапханаларға енгізілуін қатаң қадағалауға алу қажет.

Аудит жүргізу жөніндегі басшылық

Дереккөздер кодтары бар кез-келген файлға кіру бәрінен де ҰЖ оны сақтамау жолымен қорғалғаны жөн. Мұндай кодқа және қайта іріктеу және сілтемелерді қайта құру құралдарына қолжетімділік әдетте қосымшалармен қолданылатын қауіпсіздіктің ары қарай тексерісінен оңай өте алады. Өте құпия қосымшалар енгізілген өзгертулерді анықтау үшін объект кодының сомасы тексерісін растауды талап етуі мүмкін.

Сонымен қатар, өте оңай өзгертілуі мүмкін және деректердің бүтіндігінің және қолжетімділігінің жоғалуына әкелуі мүмкін, деректер базасы мен макростар есебінің бағдарламасын қарастыру қажет. Аталмыш шектеулер тек болуы мүмкін қастық әрекеттермен ғана шектелмеуі қажет, нағыз және осал ақпаратқа кіру рұқсат етілмей тұрып, өзгерістерді тестілеу және жазылуын қамтамасыз ету мақсатында қарапайым жаңартулар мен қосымшалардың бастапқы мәтінінің кодын қайта құру қатаң қадағалануы қажет. Аудиторлар құжатталған процедуралар мен жазбаларды қайта қарастыруы қажет.

6.8.5 Жасақтама ортасындағы және жұмыс ортасындағы қауіпсіздік

Мақсаты: ақпарат пен қолданбалы жүйелердің бағдарламалық құралының қауіпсіздігін қамтамасыз ету.

6.8.5.1 Өзгертулерді енгізу процессін басқару процедуралары

Өзгертулер енгізу оларды жүзеге асыру процессін басқарудың формальды процедуралары көмегімен қатаң бақылануы қажет.

Аудит жүргізу жөніндегі басшылық

Аудиторлар өзгерістерді бақылаудың формальды процедуралары жүйелік орта мен ҰЖ қосымшаларына енгізілетін барлық өзгерістер үшін қолданылатынын тексеруі қажет. Аталмыш процедуралар стандарттықтарға қарағанда сапа жөніндегі жоспарларда көбірек қажет болуы мүмкін. Сонымен қатар, мұндай процедуралардың болуын және қолдануын, ал қажеттілік жағдайында талаптарға қатысты құжаттар мен құрылым өзгерісін қамтамасыз етеді.

Атап айтқанда, онлайндық ҰЖ (көбіне ең маңызды болып табылатын) өзгерістерімен қалай жұмыс жасалатынын, олардың мұқият және кеңейтілген жоспарлауды талап ету жиілігін аңдау қажет. Апат кезінде қолдауға арналған даярламалар жеткілікті ұсынылған ба? Қызметкерлердің жүйенің маңызды бөліктеріне қолжетімділігі тек қажетті деңгейде шектелуі тиіс, бұл қалайша орындалатынын тексеру қажет. Сонымен бірге барлық өзгертулерге тиісті түрде рұқсат берілгенін (рұқсат тиісті менеджмент деңгейінен алынған және операциялық менеджмент процесске тартылған), өзгертулер дұрыс тексерілетінін және тестіленуін, өзгерістер енгізілгенге дейін толық рұқсат берілетінін тексеру керек.

Көбіне өзгертулер дайындалған жоспар бойынша алдын ала енгізілмейді, тек топталып нұсқаға орнатылады, аталмыш жағдайда нұсқалар жазбасы енгізілген өзгертулерді дұрыс сипаттағанын тексеру қажет. Жедел өзгертулерді енгізу процедурасы жүйенің бөгелу жағдайын түзету үшін қолданылуы мүмкін, мұның жоғарыда айтылған барлық талаптарға жауап беретінін тексеру қажет. Конфигурацияның сәйкес қадағалануы өзгертулер кезінде қолданылатынын, және енгізілген өзгертулер туралы дұрыс жазбалар жасалғанын тексеріңіз.

6.8.5.2 Операциялық жүйеге енгізілетін өзгерістердің техникалық талдау

Операциялық жүйеге өзгертулер енгізілген жағдайда қолданбалы жүйелердің анализі мен тестіленуі жүргізілуі қажет.

Аудит жүргізу жөніндегі басшылық

Ұйым ҰЖ өзгерулерін тексеру процедурасын жасақтауы қажет. Ол жоспарлық енгізуден бұрын жүзеге асырылуы қажет, мүмкіндігі бойынша, тестілік енгізу бағалануы қажет. Аталмыш тексеру өзгерістерден соң дайын болатын басқару элементтерін бағалауды және талаптарға сәйкестікке тексеруді қамтуы қажет. Аудиторлар өндірушілер мен нұсқаларға ескертулер деректері, олар бар болған жағдайда бағалау деректері, ҰЖ кемшіліктерінің өңделуі қолданған болса, қажет болуы мүмкін БҚ белгілі өзгерістері сияқты, тексеру туралы аталмыш есептердің мазмұнын қарауы қажет.

Аталмыш тексерулердің қорытындылары қосымшалардың кез-келген қажетті өзгерістерін және ҰЖ жаңа нұсқасын енгізу жоспарын қамтуы қажет. ҰЖ нұсқасы (сонымен бірге кез-келген бағдарламалық түзетулер)

конфигурациялық жазбаларда анықталуы қажет. Кейбір жағдайларда ұйымдар жүйені жаңартпау туралы шешім қабылдауы мүмкін, тіпті осындай жағдайлардың өзінде олардың қолдаудың жеткілікті деңгейіне қолжетімділігінің болуын қадағалау қажет, ал егер ондай қолжетімділік болмаса бұл тәуекелдерді бағалауда анықталып, сәйкес шаралардың қолдануын талап етуі қажет.

6.8.5.3 Бағдарламалар пакетіне өзгертулер енгізуге шектеу қою

Бағдарламалар пакетін түрлендіру ұсынылмайды, барлық қажетті өзгертулер қатаң қадағалануы қажет.

Аудит жүргізу жөніндегі басшылық

Өзгертулерді бақылаудың құжатталған және бекітілген процедурасын тиісті түрде қолдану қажет. Кез-келген өзгертулер бақылаумен және бұл өзгерістер толық негізделген және енгізілмес бұрын бекітілгенін кепілдей отырып, енгізілуі қажет. Бағдарламалық пакеттер осыған іскерлік талаптар қойылған шартта ғана өзгертілуі қажет.

Кейде кодтарға өзгертулер бағдарламалық түзетулер ретінде енгізіле алады, ал олар соңынан келесі нұсқаларға қосылады, егер осылай болған жағдайда, бағдарламалық түзету өшірілген ал барлық тиісті құжаттар жаңартылғанына көз жеткізу қажет. Кейде ұйымдар бағдарламалық көздерді аша алады, бірақ жасақтаушылар уәкілеттігіне ие бола алмайды; өзгертулер енгізу құқығы келісім-шарттарда нақты анықталуы қажет, бірақ өзгерістер тиісті түрде енгізілетініне көз жеткізу қажет, себебі жасақтаушылар жазбаларына толық қолжетімділіктің болмауынан жүйенің бүтіндігіне ары қарай қатерлер төндірілуі мүмкін. Сонымен қатар, түпнұсқалық бағдарламаның жаңа нұсқалары орнатылғанда, мұндай өзгерістермен қалай жұмыс жасалатынын тексеру қажет, себебі олар қайта орнатуды талап етуі мүмкін. Барлық енгізілген өзгертулердің толық тарихы сақталатынын және аталмыш жазбалар қаншалықты талап етілсе сонша сақталатынын тексеру қажет. Барлық бағдарлама-қосымшалардың өзгертілген кодтың жұмысын растау үшін қолданылуы мүмкін регрессиялық тестілердің белгілі реттілігі болуы қажет, бұл қалай қадағаланатынын байқау керек.

6.8.5.4 Жасарын арналар және «Троянский конь» типті құрама код

Бағдарламалық құралдың сатылымы, пайдалануы және түрлендіру болуы мүмкін жасырын арналар мен «Троянский конь» типті құрама кодынан қорғаныс мақсатында қатаң бақыланып, тексеріліп тұруы қажет.

Енгізу жөніндегі басшылық:

Заманауи бағдарламалық өнімдердің барлығында дерлік қандай да бір жасырын арналар бар. Олардың көбісі зиянсыз, мысалы БҚ жасақтаушы программисттер туралы ақпарат беретін арнайы кілттердің комбинациясы, бірақ олардың кейбірі қауіпті болуы мүмкін. Ұйымдар мұндай жасырын арналарға өзінің көзқарасын анықтап, олардан қорғаныс бойынша қандай да

бір әрекеттерді қолға алу қажеттігін шешуі қажет. Мұндай шешімді қабылдай отырып, жасырын арналардың ұзақ және күрделі процесстер нәтижесінде ғана анықталатынын есте сақтау қажет. «Троянский конь» типті кодтар жүйеге байқалмай енгізілуі мүмкін және алдын ала жиналған кодтарды жолдау сияқты, пайдаланушы үшін жағымсыз және байқалмайтын әрекеттерді жасау үшін қолданылуы мүмкін.

Аудит жүргізу жөніндегі басшылық

БҚ көптеген элементтерінде жасырын кодтардың әр түрлі формалары болуы мүмкін. Олардың бір бөлігі зиянсыз және ешқандай қатер төндірмейді. Ал бір жағынан олардың кейбіреулері жабық арналармен қолданылуы және оларға арналған жол ретінде пайдаланылуы мүмкін және оларды «Троянский конь» сияқты анықтау қиынға түседі.

Аудитор жасырын кодтар мен «Троянский конь» типті кодтармен күресу үшін ұйымда қандай шаралар қарастырылғанын тексеруі қажет. Жасырын арналар мен «Троянский конь» типті кодтар ақпараттың рұқсатсыз жариялануы, өзгертілуі немесе жойылуына әкелуі мүмкін екенін есте ұстау қажет.

6.8.5.5 Аутсорсинг шарттарында бағдарламалық құралды жасақтау

Аутсорсинг шарттарында орындалатын бағдарламалық құралдардың жасақтауын қорғау үшін басқару құралдары қолданылуы қажет.

Аудит жүргізу жөніндегі басшылық

Ұйым аутсорсинг шарттарында бағдарламалық құралдарды жасақтау жөніндегі қатерлерді зерттеуі қажет. Ең дұрысы жасақтау құралдары және оған кіретін процесстер инспекцияланып, тексерілуі қажет. Мұндай жасақтамаға байланысты қатерлер тексерілуі қажет, сондай-ақ кез-келген контекстте жасақтамаға кез-келген анықталған қатерлер мен аталмыш жасақтамаға қатысты, қос тараптың міндеттері мен басқару элементтерін, барлық қауіпсіздік талаптарын қамтуы қажет. Аудиторлар мұндай келісім-шарт келесі тармақтарды қамтитынына көз жеткізуі қажет:

– Уақытты шектерді және жасақталған БҚ сапасын өлшеу шарттары мен сапа кодына қойылатын талаптар;

– Орындалатын жұмыстың сапа кепілі үшін аудит жүргізу қажет болған жағдайда қолжетімділік құқығы;

– Жасақталатын БҚ тиістілігін және интеллектуалды меншік құқығын анықтаушы ережелер мен келісімдер;

– Вирустарға, жасырын арналар мен «Троянский конь» типті кодының болуына тексерумен қоса, жасақталатын кодтың жеткілікті қызмет етуін тестілеу.

6.9 Ұйымның үздіксіз жұмысын жоспарлау

6.9.1 Ұйымның үздіксіз жұмысын жоспарлау аспектілері

Мақсаты: Ұйым жұмысындағы бөгеуілдермен күресу және ірі апаттар мен катастрофалар салдарынан сындарлы өндірістік процесстердің қорғанысын қамтамасыз ету.

6.9.1.1 Ұйымның үздіксіз жұмысын жоспарлау процессі және Ұйымның үздіксіз жұмысы мен әсер ету факторларының анализі

Ұйымның барлығына үздіксіз жұмысын қамтамасыз ету жоспарларын жасақтау және жүзеге асыруға арналған ортақ қадағаланатын процесс болуы қажет.

Ұйымда үздіксіз жұмысты қамтамасыз етудің орталықтандырылған жүйесі үшін сәйкес тәуекелдерді бағалауға негізделген стратегиялық жоспар жасақталуы қажет.

Аудит жүргізу жөніндегі басшылық

Ұйымда үздіксіз жұмысын жоспарлау әр ұйымда өткізілуі қажет апаттар мен жұмыстан бөгеуден жеткілікті түрде қорғау және қатерлерді тиімді бағалау процессінің нәтижесі болып табылады. Аталмыш жоспарлардың қолдану аясы мен олардың мән-жайы қауіпсіздік талаптарына және істерді жүргізуге сәйкес келуі қажет.

Аудиторлар ұйымда үздіксіз жұмысты басқару процессінің бар екенін, ол барлық ұйымда қолданатынын тексеруі қажет.

Ұйымның үздіксіз жұмысын жоспарлау іскерлік белсенділікті бөгеу салдары және қатерлер анализіне негізделуі қажет. Аудиторлар қатерлердің бағасы тек ақпарат өңдеу қызметтеріне ғана қатысты емес, сонымен қоса іскерлік белсенділікті бөгеуге қатысты ұйымның барлық бөлімдерін қамтитынын және толық екенін тексеруі қажет. Тәуекелдердің бағалануы мен салдарының нәтижелері ұйымның үздіксіз жұмысын қамтамасыз ету жоспарын жасақтау үшін қолданылады. Аудиторлар аталмыш жоспардың қолданыс аясы мен мән-жайы аталмыш ұйымның іскерлік талаптары мен қауіпсіздігі жөніндегі талаптарға бағындырылғанын және менеджментпен қол қойылғанын айқындауы қажет.

6.9.1.2 Ұйымның үздіксіз жұмысын қамтамасыз ету жоспарларын құру және жүзеге асыру

Сындарлы өндірістік процесстердің бұзылуы немесе тоқтауы жағдайында өндірістік қызметті дер кезінде қалпына келтіру және қамтамасыз ету жөніндегі жоспарлар жасақталуы қажет.

Аудит жүргізу жөніндегі басшылық

Ұйымның үздіксіз жұмысын қамтамасыз ету жоспарлары жоғарыда сипатталғандай қауіпсіздік және бизнестің белгіленген талаптарын орындауға бағытталған болуы қажет. Аудиторлар аталмыш жоспарларға

байланысты уақытша шектер жеткілікті ме, іскерлік талаптарды қанағаттандыра ма, және олар іс жүзінде қолданыла ала ма жеген мәселелерді қарастыруы қажет. Сонымен қатар, келесіні тексеру қажет.

– Барлық міндеттемелер келісілген және бекітілген;

– Қызметкерлер апат болған немесе іскерлік белсенділік бұзылған жағдайда өз міндеттерін және өзінің не істеу қажет екенін біледі;

– Жоспарда анықталған барлық процесстер құжатталған және кестеге сәйкес енгізіледі;

– Барлық қызметкерлер апат болған немесе іскерлік белсенділік бұзылған жағдайда не істеу қажет екенін біледі;

– Жоспарлар белгіленген кестеге сәйкес тестіленеді және жаңартылады.

6.9.1.3 Ұйымның үздіксіз жұмысын қамтамасыз ету жоспарының ортақ жүйесі

Тестілеу және жүзеге асыруға арналған басымдылықтарды анықтау және барлық жоспарлардың келісілуін қамтамасыз ететін, ұйымның үздіксіз жұмысын қамтамасыз ету жоспарларының ортақ жүйесі болуы қажет.

Аудит жүргізу жөніндегі басшылық

Бірнеше бөлім немесе сценарийларға қатысты бірнеше жоспары бар барлық ұйымдарда жоспарлардың дербес шектері бар екеніне көз жеткізу қажет, аталмыш шектердің болуын және жоспарлардың оған қайшы келмейтінін тексеру қажет. Жоспарлар сонымен қоса, сервис жөніндегі міндеттіліктер деңгейіне қайшы келмеуі қажет және мұны тексеру қажет.

Жоспардың қолданысқа дайын екеніне, құжаттар тиісті түрде қадағаланатынын, және негізгі қызметкерлер алдымен не қажет екенін және қандай элементтер міндетті болып табылатынын – мысалы, сейфтер коды, апат қызметтерінің телефондары, және олардың қайда орналасқандарын т.б. білетініне көз жеткізу қажет. Қызметкерлердің таңдалуын қарастыру қажет, ұйым бір немесе бірнеше негізгі қызметкерге сүйене ме, егер олар болмаса, не болады? Сонымен қатар, төтенше жағдайларда қажет болатын ақпараттар және байланыс телефондары, қолжетімділік кодтары және т.б. жаңарту қажет пе – мұның орындалуын тексеру қажет.

Деректердің бұзылуы, вирустық шабуыл, өрт, негізгі қызметтерді жоғалту, жеткізілімдердегі ұзақ үзіліс сияқты типтік сценарийлер қарастырылды ма? Қолдаушы әрекеттерді тестілеу, деректерді қалпына келтіру, оларды өткізу және алмастыру және т.б. жөнінде нұсқамалар ба ма?

6.9.1.4 Ұйымның үздіксіз жұмысын қамтамасыз ету жоспарларын тестілеу, жүзеге асыру және жаңарту

Ұйымның үздіксіз жұмысын қамтамасыз ету жоспарлары үнемі тестіден өтіп, олардың тиімділігін арттыру мақсатында жаңартылып тұруы қажет.

Аудит жүргізу жөніндегі нұсқаулық

Ұйымның үздіксіз жұмысын қамтамасыз ету жоспарларын тестілеу міндетті болып табылады және аудиторлар жоспар аясында немесе жоспардың өзінде анықталуы мүмкін тестілеу кестесін анықтауы тиіс. Белгілі бір деңгейдегі күрделілікпен жоспарлар бірінші реттен тамаша іске қосылуы екіталай, адамдар аталмыш жағдайды сәтті игеруі үшін процедураларды қадағалауы тиіс, және бұған тек тәжірибемен ғана қол жеткізуге болады. Жоспарлардың өздерін әзірлеудің белгілі бір жоспары, толық тексеру және бірінші шығарылым алдында талқылау, кейінгі талдау және тексерумен тестілер кестесі, ұзақ жарамдылығын тексеру үшін ескертулерсіз тестілерді жүргізу және қызметкерлерді жаттықтыру үшін шарттарды беру өмір сүруі тиіс. Қандай да бір проблемалар байқалатын тестілердің нәтижелерін қарау қажет, оларға талдау жасалынды ма және түзетілді ме, қызметті бағалаудың критериялары қандай, олар сервистің тиісті деңгейіне сәйкес келді ме? Сонымен қатар тестілеуге жаңа қызметкерлер және үшінші тұлғалар енгізілді ме? соны қарау қажет. Қызметтің жалғастығы тиімді кооперацияға байланысты болуы өте жиі. Тұрақты түрде жаңғыртылмаған жоспарларға ерекше назар аударыңыз, оларды пәрменділікке тексерілуі, жаңа мүмкіндіктерді қамту, реттеуші талаптардағы өзгертулер туралы жазбалар бар ма? Жоспарларды қолдау және жаңғырту бойынша міндеттер анықталғандығын, жоспарлардағы кез келген өзгерістер тек сәйкес рұқсатпен ғана енгізіле алатындығын тексеру қажет.

6.10 Формальды талаптарға сәйкестік

6.10.1 Құқықтық талаптарды орындау

Мақсат: реттеуші міндеттемелер немесе шарттық міндеттемелер, сонымен қатар ақпараттық қауіпсіздікке қойылатын талаптар заң күшіне ие қылмыстық және азаматтық заңнаманың бұзылуынан сақтану.

6.10.1.1 Қажетті талаптарды анықтау

Қауіпсіздікке қатысы бар барлық құқықтық және шарттық талаптар айқын анықталуы және әрбір ақпараттық жүйе үшін құжатталуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Ұйым белгілі бір заңнамаға сәйкестік және анықтау үшін қабылданатын әрекеттерді аудиторларға көрсетуі тиіс. Аудиторлар бірде-бір қолданылатын заңнама ұмытылмағанын немесе қате жіберілмегенін тексеруі тиіс. Ұйымдар бұрын анықталған заңнамалық ережелерге сәйкестік үшін дайындалған басқару элементтеріне ие болуы тиіс. Басқарудың аталмыш элементтері үшін жауапкершілік анықталуы және құжатталуы тиіс, ал жауапты тұлғалар өз міндеттері жөнінде білуі тиіс.

6.10.1.2 Авторлық құқықтарды қорғау

Авторлық құқық туралы заңмен қорғалған материалдарды пайдалануға және патенттелген бағдарламамен қамтамасыз етуді пайдалануға құқықтық шектеулерді қадағалау бойынша қажетті процедуралар жүзеге асырылуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Аудиторлар ұйымдағы ақпаратқа авторлық құқықтарды және БҚ қорғау процедураларын қарауы тиіс. Аталмыш процедуралар әзірлеуге авторлық құқықтар ретінде немесе сауда маркаларымен белгіленген материалмен жұмыс істеу принциптерін сипаттауы тиіс және қызметкерлер осындай материалдармен қалай жұмыс істеуі керектігін білуі тиіс. Пайдаланушылар сонымен қатар авторлық құқықтармен қорғалған материалдарды немесе БҚ кез келген рұқсат етілмеген көшіру немесе пайдалану заңмен проблемаға әкелуі мүмкін.

Ұйымда БҚ пайдаланумен қатаң басқару элементтері қажет. Аудиторлар қандай лицензиялар иелікке алынғандығын және оларды қадағалауға қалай қолдау көрсетілетіндігін айқындауы тиіс. Көптеген коммерциялық пакеттер әртүрлі формаға ие болуы мүмкін аталмыш пакетке лицензиялық келісім болып табылады, бірегей формат өмір сүрмейді, сондықтан пайдаланушылардың саны, пайдалану бойынша шектеулер және басқалары сынды осындай ақпаратты тексеру үшін іс-әрекеттің лицензиялық келісімге сәйкестігін тексеру үшін қосымша мәліметтер жинау қажет.

Нұсқалардың бірі ұйымның осымен қалай жұмыс істегендігін қарау болып табылады, негізгі пакеттердің жинағын жинауға болады және содан кейін инвентаризациялық тексерулерден осы пайдалану туралы жазбалармен салыстыра отырып, әрбір лицензияның негізгі аспектілерін анықтайды. Әзірлеу құралдары мен кітапханаларын пайдалануды қарау қажет, олар дұрыс пайдаланды ма? Ұйым үшін әзірленген жоғарыда көрсетілген БҚ жағдайларында әзірлеуге немесе қолдауға келісім-шартты қарау қажет, егер дереккөздерге қатынау ұсынылған болса, үй өзгертулері қолданыла алады ма, БҚ пайдалану және орналасуы бойынша шектеулер өмір сүреді ме? Осыған жауапты ұйым қызметкерлері БҚ–ге авторлық құқықтарға қатысты өз міндеттемелері жөнінде толық хабардарлығына көз жеткізуі қажет. Кездейсоқ таңдап алынған персональды компьютерлерді лицензияланбаған БҚ болуына тексеріңіз.

6.10.1.3 Ұйым құжаттамасын қорғау

Ұйым үшін маңызды құжаттар жоғалудан, жойылудан және қолдан жасаудан қорғалуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Заңды немесе реттеуші мақсаттар үшін қажетті жазбалар әдетте бизнесті жүргізу үшін немесе қандай да бір басқа мақсаттарда ұйымға талап

етілетін барлық жазбалардың бір бөлігі болып табылады. Заңды немесе реттеуші мақсаттар үшін барлық қажеттінің анықталғандығына және барлық талаптарға сәйкес екендігіне көз жеткізу қажет. Бұған мысалы, қаржылық есептер, кедендік жазбалар, құқықтық жазбалар және қоршаған ортаға қатысты жазбалар ене алады. Нақтылы талаптар елге байланысты өзгеруі мүмкін және ұйым сәйкес талаптарды білуі және қадағалауы тиіс. Бұның сәйкес персоналмен орындалғанына және куәландырылғанына көз жеткізу қажет. Сақтау бойынша өкімдер (қауіпсіздікке қатысты өкімдерді қоскқанда), тексеру және иелену бойынша талаптар процедураларда анықталуы тиіс.

Қандай жазбалар енгізілгендігі жайлы нақты анықталған тізімнің қандай да бір формасы өмір сүруі тиіс және аудиторлар оның дәлдігін тексеруі тиіс. Кейбір ақпарат электронды түрде, түпнұсқа немесе сканерлеген форматта сақталуы мүмкін. Ұйым осы сақтау әдісінің заңдылығын тексергендігін және оның нақты талаптарға сәйкес келгендігін тексеру қажет.

6.10.1.4 Жеке ақпараттың құпиялылығы және деректерді қорғау

Қолданыстағы құқықтық нормаларға сәйкес жеке ақпаратты қорғау үшін бақылау құралдары қолданылуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Ұлыбританияда Деректерді Қорғау туралы Акт қадағалау үшін жеке ақпараттың нақтылы бақылауы қажет; көптеген елдерде, мысалы, Еуропада осыған ұқсас заңдар өмір сүреді. Заңнама сонымен қатар ұйымнан оның нені пайдаланатындығын тіркеуді талап етуі мүмкін және бұны тексеру қажет. Сонымен қатар пайдаланылған деректердің типін тексеру қажет, олар расталуы қажет, олар ұйым шегінен сыртқа беріледі ме? Осы деректерге кім қатынай алады, бұл олардың жұмысы үшін қажетті ме?

Ұйымның аталмыш облыстағы талаптар өзгертулерін бақылап отыратындығын тексеру қажет, жаңа, неғұрлым қатаң шектеулер орындау үшін көрсетілген мерзіммен енгізілуі мүмкін. Бұл туралы біледі ме, өзгерістерді көрсетілген уақытша рамкаларға енгізудің жоспарлары өмір сүреді ме? Аудиторлар өздері заңнаманың аталмыш аспектілері туралы толықтай хабардар болуын кепілдендіруі тиіс.

6.10.1.5 Ақпараттық ресурстарды заңсыз пайдаланудың алдын алу

Ақпараттық ресурстарды пайдалану басшылықпен санкциялануы тиіс. Бұл ресурстарды заңсыз пайдаланудан қорғау үшін сәйкес басқару құралдары қолданылуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Ақпаратты өңдеу құралдарын теріс пайдалану телефон сөйлесулерін төлеуге ұйымның жоғары шығындарын, дискілік кеңістіктің, процессор уақытының, желі жүктеуінің, жұмыс уақытын жоғалтудың және т.б. қосымша шығындарын ғана тартып қоймай, сондай-ақ маңызды ақпараттың

қасақана емес дабыралауына, бұзылуына немесе оған рұқсат етілмеген дереккөздерден қатынауға әкелуі мүмкін. Бұл сонымен қатар вирустарды, «Троя атын» жіберу және т.б. секілді БҚ қасақана зақымдалуын тартуы немесе егер аталмыш ұйымға тиесілі ақпаратты өңдеу құралдары құқыққа қарсы әрекеттерді іске асырушы қызметкерлермен пайдаланылатын болса заңнаманың бұзылуына әкелуі мүмкін. Менеджментпен анықталған және жұмыскерлермен формальды танылған және түсінілген нақты саясат өмір сүруі тиіс. Егер қызметкерлерге ойын үшін компьютерлерді, Интернетке қатынауды және т.с.с. пайдалануға рұқсат етілген жағдайда, олар маңызды ақпаратпен жұмыс істейтіндерден бөлек болуы тиіс. Принтерлер, көшірмелер және т.б. секілді қашықтағы, басқа жабдықты пайдалануды зерттеуі қажет – оларға қатысты саясат қандай?

6.10.1.6 Криптографиялық бақылау құралдарын пайдалануды регламенттеу

Криптографиялық бақылау құралдарына қатынауды регламенттеу бойынша ұлттық келісімдер, заңдар, нұсқаулар немесе басқа құжаттар талаптарын орындауды және осы құралдардың пайдаланылуын қамтамасыз ететін басқару құралдары өмір сүруі тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Ұйым аудиторларға криптографиялық басқару элементтері үшін сәйкес заңнаманы және ережелерді айқындау үшін қабылданған әрекеттерді, сонымен қатар олар қажет болғанда заңнаманы қадағалау үшін заң консультациясына жүгінгендігін көрсетуі тиіс. Аталмыш талаптарды орындау үшін пайдаланылатын басқару элементтері құжатталуы, енгізілуі және тиісті қолдау алуы тиіс. Аудитор 2.8.3 бөлімінде сипатталған криптографиялық басқару элементтерінің белгілі бір құқықтық талаптарға сәйкес келетіндігін тексеру қажет.

6.10.1.7 Дәлелдерді жинау

Егер тұлғаға немесе ұйымға бағытталған әрекеттер заңнамаға (азаматтық немесе қылмыстық) сәйкес талқылауды талап еткен жағдайда, ұсынылатын дәлелдер сәйкес заңдарда тұжырымдалған ережелерді немесе осы жағдай қаралатын нақты сот ережелерін қанағаттандыруы тиіс. Оның үстіне, рұқсат етілген дәлелдерді алу бойынша жалпы қабылданған ережелер немесе барлық жарияланған стандарттар талаптары орындалуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Дәлелдерді жинау азаматтық немесе қылмыстық құқық бұзылуының нәтижесі ретінде келуі мүмкін құқықтық процедуралар және әрекеттерді адекватты қолдау мүмкіндігі болуы үшін маңызды. Ұйым куәліктерді жинау үшін дайындалған процедураларға ие болуы және аудиторлар аталмыш процедураның келесілерді кепілдендіруін тексеруі тиіс:

– Жиналған ақпарат айғақ ретінде осындай куәліктерді беру үшін қолданылатын стандарттарға немесе тәжірибеге сәйкес;

– Аталмыш айғақтардың сапасы және толықтығы (яғни олардың салмақтылығы) жеткілікті;

– Ақпараттың толықтығы және дұрыстығы дәлелденуі мүмкін.

Аудиторлар жиналған куәліктердің қайда сақталатындығын, және аталмыш куәліктерді рұқсат етілмеген өзгертудің немесе жоюдың мүмкіндігін тексеруі тиіс. Оның үстіне, аудиторлар айғақтарды қашан жинай бастау қажеттілігі шарттарын қарастыруы тиіс. Оларды жинау ақпараттың жойылмайтындығын кепілдендіру үшін ерте кезеңде басталуы тиіс.

6.10.2 Ақпараттық жүйелердің қауіпсіздігін тексеру

Мақсат: Жүйелердің ұйымда қабылданған қауіпсіздік саясаттарына және стандарттарына сәйкестігін қамтамасыз ету.

6.10.2.1 Қауіпсіздік саясатына сәйкестік

Ұйымның басқарушы персоналы өздерінің жауапкершілігі шегіндегі қауіпсіздік процедураларының тиісті орындалуын қамтамасыз ету бойынша шараларды қабылдауы тиіс. Ұйымның барлық бөлімшелері қауіпсіздік стандарттарына және қабылданған саясатқа сәйкестікті қамтамасыз ету мақсатында тұрақты тексерілуі тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Қауіпсіздікті қамтамасыз ету бойынша процедуралар саясатының орындалу деңгейін анықтау үшін, менеджмент ішкі аудитты жүргізуді кепілдендіруі тиіс. Олар құзыретті қызметкерлермен жоспарлануы және орындалуы, толықтай құжатталуы және қадағаламауды жою үшін қадағалануы тиіс, сонымен қатар олар жөнінде басшылыққа есеп берілуі тиіс. Тексерулердің мерзімділігі қауіпсіздік талаптарына байланысты болуы тиіс және аудиторлар аталмыш жиілік тәуекел деңгейіне, ақпарат маңыздылығына, технологиялардағы өзгертулерге және ұйымға әсер етуі мүмкін кез келген басқа факторларға сәйкес келетіндігі жөніндегі мәселені қарастыруы тиіс.

6.10.2.2 Қауіпсіздік стандарттарына сәйкестікке техникалық тексеру

Ақпараттық ресурстар қауіпсіздікті қамтамасыз ету стандарттарына сәйкестікке тұрақты тексерілуі тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Ұйымдар өздерінің жүйелері қауіпсіздік және енгізу стандарттарына сәйкес келетіндігін тексеруі тиіс. Ненің тексерілетіндігін, қандай жиілікте және қандай әдістермен тексерілетіндігін көрсететін сәйкестікті тексеру жоспары өмір сүруі тиіс. Сәйкестікке тексерулердің осындай типі осы үшін жеткілікті түрде біліктілікке ие персоналмен немесе кем дегенде оның бақылауымен өткізілуі қажет. Құралдарды пайдалану жағдайында

құралдардың қандай аспектілерін олар расымен де жабатындығын бағалау қажет, бұл тек құралдардың аудиті немесе мониторинг болуы мүмкін – олар қандай да бір түрде бекітілді ме? Тексерулерді орындайтын және тексеретін қызметкерлерді тексеру қажет; көбінесе сәйкестікті тек техникалық құзыретті персонал ғана толық бағалай алады.

6.10.3 Жүйелер аудиті

Мақсат: Жүйе аудитының процесіне және аудит процесінің тарапынан әсерді азайту және тиімділікті жоғарылату.

6.10.3.1 Жүйелер аудитының құралдары

Өндірістік процестерде іркілістердің туындау тәуекелін азайту үшін жұмысшы жүйелердің аудиті жіті жоспарлануы және сәйкестендірілуі тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Жүйе аудитының құралдарын және басқару элементтерін басқару ақпараттағы және тексерілетін жүйелердегі іркілістерге әкелмеуі тиіс. Егер тексерулер жоспарланған жағдайда операциялық менеджменттен қажетті рұқсат алынғандығына куәландырылу қажет. Ақпарат аталмыш әрекеттердің мақсаттары үшін өзгертілмеуі тиіс және ақпаратқа қатынау кез келген басқа операция секілді жазылуы тиіс. Сонымен қатар іскерлік белсенділіктің үзілуі минимумға жеткізілгендігін кепілдендіру қажет. Аудит нәтижелері сақталғандығына, ал кез келген құралдарды пайдалану тиісті түрде жазылғанына көз жеткізу қажет. Сонымен қатар құралдардың өзі пайдаланудың алдында формальды түрде бекітілгендігін тексеріңіз.

6.10.3.2 Жүйелер аудитының құралдарын қорғау

Жүйелер аудитының құралдарына қатынау үздіксіз пайдаланудың кез келген мүмкіндіктерін немесе нұқсан келтірушілікті болдырмау мақсатында қорғалуы тиіс.

Аудит жүргізу жөніндегі нұсқаулық

Аталмыш құралдар маңызды ақпаратты оқу немесе өзгерту үшін пайдалану мүмкін болатын басқару элементтеріне және ақпаратқа қатынауға рұқсат береді. Бөгделердің қолында, аталмыш құралдар өте қауіпті болуы мүмкін және олардың қалай қолданылуына қатаң бақылауды жүзеге асыру қажет.

Мүмкіндігінше аталмыш құралдар операциялық және тестілеуші жүйелерден бөлек сақталуы тиіс; егер құралдар жүйеде тұрақты сақталынатын болса, қатынауды басқару құралдары қандай?

Қосымша
(анықтамалық)

Библиография

[1] БИС РД 3003:2002 «BS 7799-2 стандартына сәйкестікке аудитке дайынбыз ба» («Are you ready for a BS 7799-2 audit»);

[2] БИС РД 3004:2002 «BS 7799 стандартының басқару құралдарын іске асыру және аудиті бойынша жетекшілік» («Guide to the implementation and auditing of BS 7799 controls»).

ӘОЖ 681.324:006.354 **МСЖ 35.060**

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

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

АУДИТ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

СТ РК 34.030 - 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

Настоящий стандарт ориентирован, в основном, на сотрудников организации, ответственных за внедрение информационной безопасности, таких, как специалистов по информационной безопасности, а также лиц, занимающихся оценкой уже внедренных средств управления *СТ РК ИСО/МЭК 27001-2008*, например, для проверки степени соответствия этому стандарту, либо в целях внутреннего аудита. Руководство также может быть полезным для разработчиков в процессе настройки систем управления информационной безопасности (СУИБ) и внутренних аудиторов, проводящих оценку.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология
АУДИТ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

Дата введения 2008.07.01.

1 Область применения

Настоящий стандарт предназначен для использования в организациях, желающих самостоятельно проверить, соответствует ли их система управления информационной безопасностью (СУИБ) стандарту *СТ РК ИСО/МЭК 27001:2005,* и призван помочь организациям в подготовке к сертификации на соответствие стандарту *СТ РК ИСО/МЭК 27001,* Проверки на соответствие рекомендуется проводить под наблюдением сотрудника организации, ответственного за информационную безопасность, или силами собственных аудиторов.

Цель настоящего стандарта – предоставить организациям возможность оценить степень соответствия их СУИБ требованиям стандарта *СТ РК ИСО/МЭК 27001*. В настоящем стандарте приведена информация по подготовке и выполнению проверки на соответствие стандарту. Проверка на соответствие представляет собой заполнение анкеты.

Фактическая проверка описана в разделах 5 и 6 данного стандарта:

– Раздел 5 Оценка выполнения требований стандарта *СТ РК ИСО/МЭК 27001* – данная анкета позволяет проверить соответствие состояния организации в области информационной безопасности.

– Раздел 6 Аудит целей и средств управления, предусмотренных стандартом *СТ РК ИСО/МЭК 27001*.

Настоящий стандарт призван помочь организациям в проведении проверки их СУИБ на соответствие требованиям стандарта *СТ РК ИСО/МЭК 27001* с использованием рабочей книги для проверки процессов СУИБ с целью достичь соответствия СУИБ требованиям.

Анализ несоответствий служит лишь средством подтверждения того, что средства управления соответствуют требованиям стандарта *СТ РК ИСО/МЭК 27001*. Если некоторые средства не полностью соответствуют стандарту, организация должна документировать причины несоответствия. Аудиторы, годные к проведению оценки соответствия стандарту *СТ РК ИСО/МЭК 27001,* должны уметь анализировать эти причины и их обоснования.

Издание официальное

Следует отметить, что настоящий стандарт служит информативным пособием и не является средством определения меры соответствия стандарту *СТ РК ИСО/МЭК 27001*.

Организации могут использовать анализ несоответствий для неформальной оценки соответствия стандарту *СТ РК ИСО/МЭК 27001* перед проведением внутреннего аудита СУИБ или репетиционного аудита, выполняемого заказчиком. Анализ несоответствий не имеет формального значения для сертификации, проводимой сертифицированными специалистами, и не может использоваться при формировании утвержденного положения о применимости, поскольку он не соответствует установленным стандартом *СТ РК ИСО/МЭК 27001* требованиям к положению о применимости.

Проверка процессов СУИБ служит средством подтверждения того, что в организации имеются надлежащие системы и процессы, необходимые для выполнения требований, определенных стандартом *СТ РК ИСО/МЭК 27001*. Эта проверка должна выполняться организациями, готовящимися к сертификации, проводимой сертифицированными специалистами, а также теми, кто готовится к операциям, выполняемым после сертификации, таким как надзорный аудит, и к повторной сертификации. Она является средством, позволяющим проверить, сколько операций выполнено и сколько еще предстоит выполнить. Эта проверка не показывает, насколько хороши и эффективны были операции или насколько правильно и эффективно организована система контроля.

Важно отметить, что настоящий стандарт не рассматривает вопросы по внедрению и аудиту процессов СУИБ, которые включены в стандарт *СТ РК ИСО/МЭК 27001*.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК 1.9-2003 Государственная система стандартизации Республики Казахстан. Порядок применения международных, региональных и национальных стандартов и нормативных документов по стандартизации, метрологии, сертификации и аккредитации.

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

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

СТ РК 34.028-2008 Информационная технология. Порядок экспертизы,

---

* Применяется в соответствии СТ РК 1.9.

оценки и сертификации систем управления информационной безопасностью организации;

СТ РК 34.029-2008 Информационная технология. Оценка и управление рисками.

Руководство ИСО/МЭК 62:1996* Общие требования к органам по сертификации, проводящим сертификацию систем качества.

Руководство ИСО/МЭК 73:2002* Управление рисками. Терминология. Руководство по использованию в стандартах.

ЕА 7/03* Руководства для аккредитации органов по сертификации/регистрации систем управления информационной безопасностью.

Примечание – Должна использоваться правильная версия указанных стандартов.

3 Термины и определения

В настоящем стандарте применяются термины по Руководству ИСО/МЭК 73.

4 Область применения СУИБ

Область применения СУИБ должна быть определена четко и недвусмысленно как для организации, СУИБ которой проверяется на соответствие стандарту, так и для аудиторов.

С учетом усложнения бизнес-приложений и процессов и развития информационных систем, технологий и сетей можно разными способами очертить область применения СУИБ. Размер организации и ее территориальная разобщенность влияют на представление об адекватной области применения СУИБ. Системы для деловых применений работают автономно в редких случаях, поскольку они должны взаимодействовать с другими системами. Таким образом, при определении области применения СУИБ необходимо принимать во внимание все связи с другими системами и процессами за пределами данной СУИБ.

Рекомендации по выявлению и определению области применения СУИБ изложены в настоящем стандарте, в котором разъясняется определение, приведенное в стандарте *СТ РК ИСО/МЭК 27001*. В стандарте область применения СУИБ описывается в терминах организации, ее местоположения, ресурсов и технологии. Для более полного понимания необходимо добавить к этому информационные ресурсы, бизнес-приложения и процессы, а также используемую технологию. Нет необходимости детально определять эти элементы, однако важно выявить все значимые ресурсы.

5 Оценка выполнения требований стандарта *СТ РК ИСО/МЭК 27001*

Таблица 1 предназначена для получения оценок выполнения норм основной части стандарта *СТ РК ИСО/МЭК 27001*. Если одна из ячеек в графе Частично или Нет была отмечена галочкой, необходимо указать причины и обоснование в ячейках таблицы 1.

Таблица 2 предназначена для получения оценки выполнения требований Приложения А стандарта ИСО/МЭК 27001.

Таблица 1 – Оценка соответствия требованиям разделов стандарта *СТ РК ИСО/МЭК 27001*

Проверяемое требование стандарта	**Оценка выполнения требования стандарта**			**Рекомендации по выполнению требования стандарта**
	ДА (выполняется полностью)	**ЧАСТИЧНО (выполняется частично)**	**НЕТ (не выполняется)**	
4.2 Создание и управление СУИБ				
4.2.1 Создание СУИБ ***Организация должна:***				
а) Определить область применения и границы СУИБ в терминах характеристик бизнеса, организации, ее местонахождения, активов и технологий, при этом должно быть приведено подробное обоснование для всех исключений из области применения (см. ИСО/МЭК 27001:2005, 1.2)				
4.2.1.а.1 Существует ли документ, однозначно определяющий область применения и границы СУИБ?				
4.2.1.а.2 Содержит ли указанное определение информацию о характеристиках бизнеса, организации, ее местонахождения, активов и технологий?				
4.2.1.а.3 Идентифицированы ли существенные исключения из области применения, и дано ли четкое объяснение и обоснование указанных исключений?				
б) Определить политику СУИБ в терминах характеристик бизнеса, организации, ее местонахождения, ресурсов и технологий.				
4.2.1.б.1 Определена ли политика СУИБ, охватывающая заданную область применения СУИБ?				
4.2.1.б.2 Включает ли указанная политика общую структуру для определения целей и задает ли она общие задачи руководства и принципы деятельности в отношении информационной безопасности?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
4.2.1.б.3 Учитывает ли эта политика производственные и правовые или нормативные требования, а также договорные обязательства по безопасности?				
4.2.1.б.4 Учитывает ли эта политика контекст управления стратегическими рисками организации, в котором будут осуществляться разработка и сопровождение СУИБ?				
4.2.1.б.5 Устанавливает ли эта политика критерии, по которым будет определяться уровень рисков (см. 4.2.1в))?				
4.2.1.б.6 Была ли эта политика утверждена руководством?				
в) Определить подход организации к оценке рисков.				
4.2.1.в.1 Идентифицирован ли метод оценки рисков, который соответствует используемой СУИБ, идентифицированным требованиям к безопасности бизнес-информации, а также правовым и нормативным требованиям?				
4.2.1.в.2 Разработаны ли критерии для принятия рисков и определения приемлемых уровней рисков (см. 5.1.f)?				
4.2.1.в.3 Гарантирует ли выбранный метод оценки рисков сопоставимые и воспроизводимые результаты процедуры оценки рисков?				
г) Идентифицировать риски				
4.2.1.г.1 Разработан и используется ли процесс для идентификации рисков?				
4.2.1.г.2 Идентифицирует ли указанный процесс активы, относящиеся к области применения СУИБ, и владельцев этих активов?				
4.2.1.г.3 Идентифицирует ли этот процесс угрозы этим ресурсам?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
4.2.1.г.4 Идентифицирует ли этот процесс уязвимости, которые могут быть использованы для реализации этих угроз?				
4.2.1.г.5 Идентифицирует ли этот процесс воздействие, которое могут оказать на активы нарушения конфиденциальности, целостности и доступности?				
д) Проанализировать и оценить риски				
4.2.1.д.1 Разработан и используется ли процесс для анализа и оценки рисков?				
4.2.1.д.2 Оценивает ли указанный процесс в масштабе организации воздействия на бизнес, которые могут оказать нарушения безопасности, с учетом последствий нарушения конфиденциальности, целостности или доступности ресурсов?				
4.2.1.д.3 Оценивает ли указанный процесс реальную вероятность реализации нарушений безопасности в свете превалирующих угроз, уязвимостей и воздействий, связанных с этими ресурсами, а также реализованных на данный момент средств управления?				
4.2.1.д.4 Оценивает ли указанный процесс уровни рисков?				
4.2.1.д.5 Определяет ли указанный процесс, являются ли риски приемлемыми или требуют обработки, используя критерии принятия рисков, определенные в 4.2.1.в)2)?				
е) Идентифицировать и оценить варианты обработки рисков				
4.2.1.е.1 Разработан и используется ли процесс для идентификации и оценки вариантов обработки рисков?				
4.2.1.е.2 Рассматриваются ли в указанном процессе следующие возможные действия:				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
1) применение надлежащих средств управления; 2) сознательное и намеренное принятие рисков, при условии, что они явно удовлетворяют политикам организации и критериям принятия рисков (см. 4.2.1.в).2); 3) предотвращение рисков или 4) передача ассоциированных бизнес-рисков другим сторонам, например, страховщикам и поставщикам?				
ж) Выбрать цели управления и средства управления для обработки рисков				
4.2.1.ж.1 Разработан и используется ли процесс для выбора и внедрения целей управления и средств управления, удовлетворяющих требованиям, идентифицированным при оценке рисков и в процессе обработки рисков?				
4.2.1.ж.2 Учитывает ли указанный процесс выбора критерии принятия рисков (см. 4.2.1в)), а также правовые и нормативные требования, договорные обязательства?				
4.2.1.ж.3 Гарантирует ли указанный процесс выбора, что цели управления и средства управления выбираются из Приложения А стандарта ИСО/МЭК 27001:2005, и что они позволяют выполнить все идентифицированные требования?				
4.2.1.ж.4 Допускает ли указанный процесс выбора выбор целей управления и средств управления не из Приложения А стандарта ИСО/МЭК 27001:2005?				
з) Получить у руководства утверждение предлагаемых остаточных рисков				
4.2.1.з.1 Разработан и используется ли процесс для получения у руководства утверждения остаточных рисков?				
и) Получить разрешение руководства на реализацию и эксплуатацию СУИБ				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	**ЧАСТИЧНО (выполняется частично)**	**НЕТ (не выполняется)**	
4.2.1.и.1 Разработан и используется ли процесс для получения разрешение руководства на реализацию и эксплуатацию СУИБ?				
к) Подготовить «Положение о применимости целей и средств управления СУИБ»				
4.2.1.к.1 Разработан и используется ли процесс для подготовки «Положения о применимости ...»?				
4.2.1.к.2 Подготовлено ли «Положение о применимости ...», включающее в себя цели управления и средства управления, выбранные в 4.2.1.ж, а также причины их выбора?				
4.2.1.к.3 Включает ли указанное «Положение о применимости ...» цели управления и средства управления, реализованные на текущий момент?				
4.2.1.к.4 Зарегистрировано ли в указанном «Положении о применимости ...» исключение любой из целей управления и любого из средств управления, перечисленных в Приложении А стандарта ИСО/МЭК 27001:2005, а также обоснование исключения этих целей и средств?				
4.2.2 Реализация и эксплуатация СУИБ ***Организация должна:***				
а) Сформулировать положения плана обработки рисков, в котором идентифицируются соответствующие действия руководства, активы, обязанности и приоритеты для управления рисками информационной безопасности (см. 5).				
4.2.2.а.1 Разработан ли и используется ли процесс формулирования плана обработки рисков, в котором идентифицируются соответствующие действия руководства, обязанности и приоритеты для управления рисками информационной безопасности?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
4.2.2.а.2 Обеспечивает ли указанный процесс идентификацию необходимых действий руководства в плане обработки рисков?				
4.2.2.а.3 Обеспечивает ли указанный процесс идентификацию необходимых обязанностей и приоритетов для управления рисками информационной безопасности (см. раздел 5)?				
б) Реализовать план обработки рисков, чтобы достичь идентифицированных целей управления, что включает в себя рассмотрение вопросов финансирования, распределения ролей и ответственности.				
4.2.2.б.1 Разработан и используется ли процесс для реализации плана обработки рисков?				
4.2.2.б.2 Позволяет ли указанный процесс гарантировать, что реализованный план обработки рисков обеспечит достижение идентифицированных целей управления?				
4.2.2.б.3 Включает ли указанный процесс рассмотрение вопросов финансирования, распределения ролей и ответственности?				
в) Реализовать средства управления, выбранные в 4.2.1.ж, для выполнения целей управления.				
4.2.2.в.1 Разработан и используется ли процесс внедрения средств управления, выбранных в 4.2.1.ж?				
4.2.2.в.2 Обеспечивает ли данный процесс соответствие внедряемых средств управления целям управления?				
г) Определить, как измерить эффективность выбранных средств управления или групп средств управления и указать, как эти измерения должны использоваться для оценки эффективности средств управления, чтобы получаемые результаты были сопоставимыми и воспроизводимыми (см. 4.2.3.в))				
4.2.2.г.1 Разработан ли и используется ли процесс, позволяющий определить, как измерить эффективность выбранных средств управления или групп средств управления?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	**ЧАСТИЧНО (выполняется частично)**	**НЕТ (не выполняется)**	
4.2.2.г.2 Содержит ли данный процесс указания, как должны использоваться эти измерения для оценки эффективности средств управления или групп средств управления?				
4.2.2.г.3 Обеспечивает ли указанный процесс получение сопоставимых и воспроизводимых результатов измерений (см. 4.2.3.в)?				
д) Реализовать программы обучения и оповещения (см. 5.2.2)				
4.2.2.д Разработан и используется ли процесс для реализации необходимых программ обучения и оповещения (в соответствии с 5.2.2)?				
е) Управлять эксплуатацией СУИБ				
4.2.2.е Разработан и используется ли процесс для управления эксплуатацией СУИБ?				
ж) Управлять ресурсами для СУИБ (см. 5.2)				
4.2.2.ж Разработан и используется ли процесс для управления ресурсами, необходимыми для СУИБ (в соответствии с 5.2)?				
з) Реализовать процедуры и другие средства управления, позволяющие обеспечить незамедлительное обнаружение событий безопасности и реагирование на инциденты безопасности (см. 4.2.3.а)				
4.2.2.з Разработан ли процесс для реализации процедур и других средств управления, позволяющих обеспечить незамедлительное обнаружение событий безопасности и реагирование на инциденты безопасности (см. 4.2.3)?				
4.2.3 Мониторинг и анализ СУИБ ***Организация должна:***				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
а) Выполнять процедуры мониторинга и анализа процедур и других средств управления				
4.2.3.а.1 Разработан и используется ли процесс мониторинга и анализа процедур и других средств управления, позволяющих выполнять мониторинг и анализ ошибок, нарушений безопасности и инцидентов безопасности?				
4.2.3.а.2 Обеспечивает ли указанный процесс своевременное обнаружение ошибок в результатах обработки?				
4.2.3.а.3 Обеспечивает ли указанный процесс своевременную идентификацию неудавшихся и успешных нарушений безопасности и инцидентов безопасности?				
4.2.3.а.4 Предоставляет ли указанный процесс возможность руководству определять, выполняются ли надлежащим образом действия по обеспечению безопасности, порученные людям или реализованные средствами информационных технологий?				
4.2.3.а.5 Помогает ли указанный процесс выявлять события безопасности и, таким образом, предотвращать инциденты безопасности путем использования индикаторов?				
4.2.3.а.6 Позволяет ли указанный процесс определить, эффективны ли действия, предпринятые для устранения нарушения безопасности?				
б) Осуществлять регулярный анализ эффективности СУИБ (включая соблюдение политики СУИБ и целей безопасности, а также анализ средств управления безопасностью) с учетом результатов аудитов безопасности, инцидентов, результатов измерений эффективности, предложений и информации, полученной от всех заинтересованных сторон				
4.2.3.б.1 Разработан ли и используется ли процесс для регулярного анализа эффективности СУИБ?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
4.2.3.б.2 Включает ли данный процесс анализ соблюдения политики безопасности и целей управления, а также анализ средств управления безопасностью?				
4.2.3.б.3 Учитывает ли указанный процесс результаты аудитов безопасности, инциденты, результаты измерений эффективности, предложения и информацию, полученные от всех заинтересованных сторон?				
в) Измерять эффективность средств управления, чтобы убедиться в том, что требования безопасности удовлетворяются.				
4.2.3.в.1 Разработан ли процесс для измерения эффективности средств управления?				
4.2.3.в.2 Обеспечивает ли указанный процесс проверку выполнения идентифицированных требований безопасности?				
г) Осуществлять анализ оценок рисков через запланированные периоды и анализировать уровень остаточных рисков и идентифицированные приемлемые уровни рисков				
4.2.3.г.1 Разработан и используется ли процесс анализа оценок рисков через запланированные периоды, а также анализа уровня остаточных рисков и идентифицированных приемлемых уровней рисков?				
4.2.3.г.2 Учитывает ли указанный процесс изменения, происходящие в организации?				
4.2.3.г.3 Учитывает ли указанный процесс изменения, происходящие в технологии?				
4.2.3.г.4 Учитывает ли указанный процесс изменения, происходящие в бизнес-целях и бизнес-процессах?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
4.2.3.г.5 Учитывает ли указанный процесс идентифицированные угрозы?				
4.2.3.г.6 Учитывает ли указанный процесс эффективность реализованных средств управления?				
4.2.3.г.7 Учитывает ли указанный процесс внешние события, такие как изменения в правовой или нормативной области, изменения договорных обязательств и изменения в общественном климате?				
д) Проводить внутренние аудиты СУИБ через запланированные периоды (см. Раздел 6 Стандарта)				
4.2.3.д Разработан ли процесс, обеспечивающий проведение внутренних аудитов СУИБ через запланированные периоды (в соответствии с п. 6 Стандарта)				
е) Регулярно проводить анализ СУИБ управленческим персоналом, чтобы гарантировать, что область применения остается адекватной, а усовершенствования процесса СУИБ идентифицированы (см. 7.1 Стандарта).				
4.2.3.е Разработан и используется ли процесс для регулярного анализа СУИБ управленческим персоналом, позволяющий гарантировать сохранение адекватности области применения и идентификацию усовершенствований процесса СУИБ (в соответствии с 7.1 Стандарта)?				
ж) Обновлять планы по безопасности, чтобы учесть сведения, полученные в результате мониторинга и анализа				
4.2.3.ж Разработан и используется ли процесс для обновления планов по безопасности, позволяющий учесть сведения, полученные в результате мониторинга и анализа?				
з) Регистрировать действия и события, которые могут повлиять на эффективность или производительность СУИБ (см. 4.3.3 Стандарта)				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	**ЧАСТИЧНО (выполняется частично)**	**НЕТ (не выполняется)**	
4.2.3.з Разработан и используется ли процесс для регистрации действий и событий, которые могут повлиять на эффективность или производительность СУИБ (в соответствии с 4.3.3 Стандарта)?				
4.2.4 Сопровождение и совершенствование СУИБ ***Организация должна регулярно:***				
а) Реализовывать идентифицированные усовершенствования СУИБ				
4.2.4.а Разработан и используется ли процесс для реализации идентифицированных усовершенствований в СУИБ?				
б) Принимать надлежащие корректирующие и превентивные меры в соответствии с пунктами 8.2 и 8.3 Стандарта				
4.2.4.б.1 Разработан и используется ли процесс для принятия необходимых корректирующих и предупреждающих мер, в соответствии с пунктами 8.2 и 8.3?				
4.2.4.б.2 Разработан и используется ли процесс для применения знаний, полученных из опыта обеспечения безопасности, имеющегося как у других организаций, так и у самой организации?				
в) Информировать все заинтересованные стороны о мерах и усовершенствованиях (уровень детальности сообщений должен соответствовать обстоятельствам), а также согласовывать с ними предполагаемые действия				
4.2.4.в.1 Разработан и используется ли процесс для информирования всех заинтересованных сторон о мерах и усовершенствованиях?				
4.2.4.в.2 Обеспечивает ли указанный процесс надлежащий уровень детальности информирования?				
4.2.4.в.3 Включает ли указанный процесс процедуры для согласования предполагаемых действий?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
г) Удостоверяться, что усовершенствования достигают поставленных целей				
4.2.4.г Разработан и используется ли процесс, позволяющий убедиться, что усовершенствования достигают поставленных целей?				
4.3 Требования к документации				
4.3.1 Общие требования				
4.3.1.а Включает ли документация записи управленческих решений, гарантирует ли она прослеживаемость связи действий с управленческими решениями и политиками и обеспечивает ли воспроизводимость записанных результатов?				
4.3.1.б Имеется ли возможность продемонстрировать взаимосвязи от выбранных средств управления назад к результатам оценки рисков и процесса обработки рисков, и далее до политики СУИБ и целей?				
4.3.1.в Содержит ли документация СУИБ документированные положения политики безопасности (см. 4.2.1.б) и цели управления?				
4.3.1.г Существует ли документ, описывающий область применения СУИБ (см. 4.2.1.а)?				
4.3.1.д Включает ли документация по СУИБ процедуры и средства управления, используемые для поддержки СУИБ?				
4.3.1.е Включает ли документация по СУИБ описание методологии оценки рисков (см. 4.2.1.в)?				
4.3.1.ж Входит ли в документацию по СУИБ отчет об оценке рисков (см. 4.2.1.в – 4.2.1.ж)?				
4.3.1.з Включен ли в документацию по СУИБ план обработки рисков (см. 4.2.2.б)?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
4.3.1.и Доступны ли документированные процедуры, необходимые организации для обеспечения эффективного планирования, эксплуатации и управления своими процессами информационной безопасности и для описания способа измерения эффективности средств управления (см. 4.2.3.в)?				
4.3.1.к Доступны ли записи, требуемые стандартом ИСО/МЭК 27001:2005 (см. также 4.3.3)?				
4.3.1.л Включено ли Положение о применимости в документацию по СУИБ?				
4.3.2 Управление документами				
4.3.2.а Разработан и используется ли процесс для защиты и управления документами, необходимыми для СУИБ?				
4.3.2.б Была ли разработана процедура для поддержки указанного процесса и определения управляющих воздействий для управления документами?				
4.3.2.в Определяет ли указанная процедура действия, необходимые для утверждения документов по критерию их адекватности перед публикацией документов?				
4.3.2.г Включает ли указанная процедура анализ и обновление документов по мере необходимости и повторное утверждение документов?				
4.3.2.д Обеспечивает ли указанная процедура идентификацию изменений и статуса текущей редакции документов?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
4.3.2.е Обеспечивает ли указанная процедура доступность важных версий соответствующих документов в местах их использования?				
4.3.2.ж Обеспечивает ли указанная процедура сохранение удобочитаемости и быстрой идентификации документов?				
4.3.2.з Обеспечивает ли указанная процедура доступность документов для тех, кому они требуются, а также передачу, хранение и, наконец, уничтожение документов согласно процедурам, применяемым в соответствии с классификацией документов?				
4.3.2.и Обеспечивает ли указанная процедура идентификацию документов внешнего происхождения?				
4.3.2.к Обеспечивает ли указанная процедура контроль над распространением документов?				
4.3.2.л Предотвращает ли указанная процедура случайное использование устаревших документов?				
4.3.2.м Обеспечивает ли указанная процедура удобную идентификацию документов, если они сохраняются для каких-либо целей?				
4.3.3 Управление записями				
4.3.3.а Разработан ли и используется ли процесс для создания и поддержки записей, обеспечивающих свидетельства соответствия требованиям и эффективной эксплуатации СУИБ?				
4.3.3.б Обеспечивает ли указанный процесс защищенность и управление записями?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
4.3.3.в Гарантирует ли указанный процесс, что в СУИБ учитываются все важные правовые и нормативные требования, а также договорные обязательства?				
4.3.3.г Обеспечивает ли указанный процесс удобочитаемость, легкость идентификации и извлечения записей?				
4.3.3.д Задокументированы ли и реализованы ли средства управления, необходимые для идентификации, хранения, защиты, извлечения и уничтожения записей?				
4.3.3.е Ведутся ли записи производительности процессов, определенных в 4.2, и записи всех случаев важных инцидентов безопасности, связанных с СУИБ?				
5 Ответственность руководства (управляющего персонала)				
5.1 Приверженность руководства				
5.1.а Разработан и используется ли процесс, позволяющий руководству продемонстрировать свою приверженность (заинтересованность) к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?				
5.1.б Включает ли указанный процесс участие руководства в разработке Политики СУИБ?				
5.1.в Обеспечивает ли указанный процесс участие руководства в разработке целей и планов СУИБ?				
5.1.г Включает ли указанный процесс распределение (руководством) ролей и ответственности за информационную безопасность?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
5.1.д Включает ли указанный процесс информирование (руководством) сотрудников организации о важности достижения целей информационной безопасности и соблюдения политики информационной безопасности, ответственности организации перед законом и необходимости постоянного совершенствования?				
5.1.е Включает ли указанный процесс предоставление (руководством) достаточных ресурсов для разработки, реализации, эксплуатации, сопровождения и совершенствования СУИБ (в соответствии с 5.2.1 Стандарта)?				
5.1.ж Включает ли указанный процесс участие руководства в выборе критериев для принятия рисков и приемлемых уровней рисков?				
5.1.з Обеспечивает ли указанный процесс обеспечение проведения внутренних аудитов СУИБ (в соответствии с п. 6)?				
5.1.и Включает ли указанный процесс проведение управленческого анализа СУИБ (в соответствии с п. 7)?				
5.2 Управление ресурсами				
Требование 5.2.1 Предоставление ресурсов				
5.2.1.а Разработан ли процесс, который используется организацией для определения и предоставления ресурсов, необходимых для СУИБ?				
5.2.1.б Обеспечивает ли указанный процесс предоставление ресурсов, необходимых для разработки, реализации, эксплуатации, мониторинга, анализа, сопровождения и совершенствования СУИБ?				
5.2.1.в Обеспечивает ли указанный процесс предоставление ресурсов, необходимых для обеспечения поддержки бизнес-требований процедурами информационной безопасности?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
5.2.1.г Обеспечивает ли указанный процесс предоставление ресурсов, необходимых для идентификации и учета правовых и нормативных требований, а также договорных обязательств по безопасности?				
5.2.1.д Обеспечивает ли указанный процесс предоставление ресурсов, необходимых для обеспечения адекватной безопасности с помощью корректного применения всех реализованных средств управления?				
5.2.1.е Обеспечивает ли указанный процесс предоставление ресурсов, необходимых для выполнения анализа по мере необходимости и надлежащего реагирования по результатам анализа?				
5.2.1.ж Обеспечивает ли указанный процесс предоставление ресурсов, необходимых для совершенствования, если требуется, эффективности СУИБ?				
Требование 5.2.2 Обучение, осведомленность и компетентность				
5.2.2.а Разработан и используется ли процесс, гарантирующий, что весь персонал, на который возложены обязанности, определенные в СУИБ, имеет надлежащую квалификацию для выполнения необходимых задач?				
5.2.2.б Обеспечивает ли указанный процесс определение необходимого уровня квалификации персонала, выполняющего работы, связанные с СУИБ?				
5.2.2.в Обеспечивает ли указанный процесс проведение обучения или принятие других мер (например, найма квалифицированного персонала) для удовлетворения этих потребностей?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
5.2.2.г Включает ли указанный процесс действия по оценке эффективности принятых мер?				
5.2.2.д Обеспечивает ли указанный процесс ведение записей об образовании, обучении, навыках, опыте и квалификации (в соответствии с 4.3.3 Стандарта)?				
5.2.2.е Разработан и используется ли процесс, позволяющий гарантировать осведомленность всего задействованного персонала о значимости и важности его деятельности по обеспечению информационной безопасности, а также о его участии в достижении целей СУИБ?				
6 Внутренние аудиты СУИБ				
6.а Разработан и используется ли процесс, обеспечивающий проведение внутренних аудитов СУИБ через запланированные интервалы времени?				
6.б Позволяет ли данный процесс определить, соответствуют ли цели управления, средства управления, процессы и процедуры СУИБ требованиям стандарта ИСО/МЭК 27001:2005 и соответствующим законам и нормативам?				
6.в Позволяет ли данный процесс определить, соответствуют ли цели управления, средства управления, процессы и процедуры СУИБ идентифицированным требованиям информационной безопасности?				
6.г Позволяет ли данный процесс определить, эффективно ли реализуются и сопровождаются цели управления, средства управления, процессы и процедуры СУИБ?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
6.д Позволяет ли данный процесс определить, выполняются ли цели управления, средства управления, процессы и процедуры в соответствии с ожиданиями?				
6.е Спланирована ли программа аудита, учитывающая статус и важность подлежащих аудиту процессов и областей, а также результаты предыдущих аудитов?				
6.ж Разработан и используется ли процесс, обеспечивающий определение критериев, границ, периодичности и методов аудита?				
6.з Разработан и используется ли процесс для выбора аудиторов, гарантирующий объективность и беспристрастность процесса аудита и невозможность аудиторам проводить аудит своей собственной работы?				
6.и Разработана и используется ли документированная процедура, определяющая обязанности и требования к планированию и проведению аудита, а также к отчетности и ведению записей по результатам аудита (в соответствии с 4.3.3 Стандарта)?				
6.к Разработан и используется ли процесс, обеспечивающий незамедлительное принятие мер со стороны управленческого персонала, ответственного за подлежащую аудиту область, по устранению обнаруженных несоответствий и их причин?				
6.л Разработан и используется ли процесс, гарантирующий, что последующие действия (follow-up activities) будут включать проверку принятых мер и составление отчета по результатам проверки в соответствии с п. 8 Стандарта?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
7 Пересмотр (анализ) СУИБ руководством				
7.1 Общие положения				
7.1.а Разработан и используется ли процесс, гарантирующий проведение анализа СУИБ через запланированные интервалы времени (не реже одного раза в год) с целью обеспечить ее постоянную применимость, адекватность и эффективность?				
7.1.б Включает ли указанный анализ определение возможностей совершенствования и необходимости изменения СУИБ, в том числе политики информационной безопасности и целей информационной безопасности?				
7.1.в Документируются ли результаты анализа в явном виде, и ведутся ли соответствующие записи (в соответствии с 4.3.3)?				
7.2 Исходные данные для анализа				
7.2.а Разработан и используется ли процесс, позволяющий включить всю необходимую информацию в исходные данные для анализа руководством (управленческого анализа)?				
7.2.б Обеспечивает ли указанный процесс использование результатов аудитов и анализа СУИБ в качестве исходных данных для управленческого анализа?				
7.2.в Обеспечивает ли указанный процесс использование замечаний и предложений заинтересованных сторон в качестве исходных данных для управленческого анализа?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
7.2.г Обеспечивает ли указанный процесс использование информации о методах, продуктах или процедурах, которые могут быть использованы в организации для повышения производительности и эффективности СУИБ, в качестве исходных данных для управленческого анализа?				
7.2.д Обеспечивает ли указанный процесс включение информации о статусе превентивных и корректирующих мер в исходные данные для управленческого анализа?				
7.2.е Обеспечивает ли указанный процесс использование информации об уязвимостях или угрозах, не учтенных адекватным образом при предыдущей оценке рисков, в качестве исходных данных для управленческого анализа?				
7.2.ж Обеспечивает ли указанный процесс использование результатов измерения эффективности в качестве исходных данных для управленческого анализа?				
7.2.з Обеспечивает ли указанный процесс использование информации о мерах, принятых по результатам предыдущего управленческого анализа, в качестве исходных данных для управленческого анализа?				
7.2.и Обеспечивает ли указанный процесс использование информации обо всех изменениях, которые могли повлиять на СУИБ, в качестве исходных данных для управленческого анализа?				
7.2.к Обеспечивает ли указанный процесс использование рекомендаций по совершенствованию в качестве исходных данных для управленческого анализа?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
7.3 Итоги анализа				
7.3.а Разработан и используется ли процесс, позволяющий включить в итоги управленческого анализа все необходимые решения и меры, связанные с управленческим анализом СУИБ?				
7.3.б Обеспечивает ли указанный процесс включение всех необходимых решений и мер повышением эффективности СУИБ, связанных с, в итоги управленческого анализа?				
7.3.в Обеспечивает ли указанный процесс включение всех необходимых решений и мер, связанных с обновлением оценки рисков и плана обработки рисков, в итоги управленческого анализа?				
7.3.г Обеспечивает ли указанный процесс включение всех необходимых решений и мер, связанных с модификацией процедур и средств управления, воздействующих на информационную безопасность, в итоги управленческого анализа?				
7.3.д Включает ли указанная модификация процедур и средств управления, воздействующих на информационную безопасность, реагирование на внутренние и внешние события, которые могут повлиять на СУИБ, в том числе изменения в: i) бизнес-требованиях; ii) требованиях безопасности; iii) бизнес-процессах, влияющих на существующие бизнес-требования; iv) нормативных или правовых требованиях; v) договорных обязательствах и vi) уровнях риска и/или критериях принятия рисков?				
7.3.е Обеспечивает ли указанный процесс включение всех необходимых решений и мер, связанных с определением потребностей в ресурсах, в итоги управленческого анализа?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
7.3.ж Обеспечивает ли указанный процесс включение всех необходимых решений и мер, связанных с совершенствованием существующих способов измерения эффективности средств управления, в итоги управленческого анализа?				
8 Совершенствование СУИБ				
8.1 Постоянное совершенствование				
8.1.а Разработан и используется ли процесс, обеспечивающий постоянное повышение эффективности СУИБ организацией путем использования политики информационной безопасности, целей информационной безопасности, результатов аудитов, анализа отслеживаемых событий, корректирующих и превентивных воздействий, а также управленческого анализа (в соответствии с п. 7 Стандарта)?				
8.2 Корректирующее воздействие				
8.2.а Разработан и используется ли процесс, обеспечивающий принятие мер для устранения причин несоответствий требованиям СУИБ, чтобы предотвратить повторное появление несоответствий?				
8.2.б Разработана и используется ли документированная процедура для корректирующих воздействий?				
8.2.в Обеспечивает ли указанная процедура идентификацию несоответствий?				
8.2.г Обеспечивает ли указанная процедура определение причин несоответствий?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
8.2.д Обеспечивает ли указанная процедура оценку необходимости воздействий, исключающих возможность повторного появления несоответствий?				
8.2.е Обеспечивает ли указанная процедура определение и реализацию необходимых корректирующих воздействий?				
8.2.ж Обеспечивает ли указанная процедура регистрацию результатов предпринятых воздействий (в соответствии с 4.3.3)?				
8.2.з Обеспечивает ли указанная процедура анализ предпринятых корректирующих воздействий?				
8.3 Предупреждающее воздействие				
8.3.а Разработан ли и используется ли процесс, позволяющий определить меры для исключения причин возможных несоответствий требованиям СУИБ, чтобы предотвратить появление несоответствий?				
8.3.б Обеспечивает ли указанный процесс адекватность принимаемых предупреждающих мер степени воздействия потенциальных проблем?				
8.3.в Разработана и используется ли документированная процедура для предупреждающих воздействий?				
8.3.г Обеспечивает ли указанная процедура идентификацию потенциальных несоответствий и их причин?				
8.3.д Обеспечивает ли указанная процедура оценку необходимости воздействия для предотвращения появления несоответствий?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
8.3.е Обеспечивает ли указанная процедура определение и реализацию необходимого предупреждающего воздействия?				
8.3.ж Обеспечивает ли указанная процедура регистрацию результатов предпринятого воздействия (в соответствии с 4.3.3)?				
8.3.з Обеспечивает ли указанная процедура анализ предпринятого предупреждающего воздействия?				
8.3.и Разработан ли и используется ли процесс, позволяющий организации идентифицировать изменившиеся риски и требования к предупреждающим воздействиям, уделяя особое внимание значительно изменившимся рискам?				
8.3.к Разработан ли и используется ли процесс, обеспечивающий определение приоритета предупреждающих воздействий на основании результатов оценки рисков?				

Таблица 2 – Приложение А стандарта ИСО/МЭК 27001:2005

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	**ЧАСТИЧНО (выполняется частично)**	**НЕТ (не выполняется)**	
А.5 Политика безопасности				
А.5.1 Политика информационной безопасности ***Организация должна:***				
Обеспечить для информационной безопасности управление и поддержку со стороны управленческого персонала согласно бизнес-требованиям и соответствующим законам и нормативам.				
А.5.1.1. Был ли документ о политике информационной безопасности утвержден руководством организации, опубликован и доведен до сведения всех сотрудников и релевантных внешних сторон?				
А.5.1.2 Проводится ли анализ политики информационной безопасности через запланированные периоды времени или в случае появления существенных изменений, чтобы обеспечить ее постоянную применимость, адекватность и эффективность?				
А.6 Организационные аспекты информационной безопасности				
А.6.1 Внутренние организационные аспекты ***Организация должна:***				
Управлять информационной безопасностью в организации.				
А.6.1.1 Обеспечивает ли руководство активную поддержку безопасности в организации путем прямого указания, демонстрации заинтересованности, прямого назначения и признания ответственности за информационную безопасность?				
А.6.1.2 Скоординирована ли деятельность по информационной безопасности представителями различных частей организации с соответствующими ролями и рабочими функциями?				
А.6.1.3 Было ли проведено четкое определение обязанностей по обеспечению информационной безопасности?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.6.1.4 Был ли определен и реализован процесс утверждения руководством новых средств обработки информации?				
А.6.1.5 Были ли идентифицированы требования к соглашениям о конфиденциальности или неразглашении, отражающие потребности организации в защите информации, и осуществляется ли регулярный пересмотр этих требований?				
А.6.1.6 Поддерживаются ли надлежащие контакты с соответствующими уполномоченными организациями?				
А.6.1.7 Поддерживаются ли надлежащие контакты со специализированными группами или другими форумами специалистов по информационной безопасности и профессиональными объединениями?				
А.6.1.8 Проводится ли через запланированные интервалы времени или в случае значительных изменений в реализации безопасности независимый анализ подхода организации к управлению информационной безопасностью, а также анализ реализации этого подхода (т.е. целей управления, средств управления, политик, процессов и процедур информационной безопасности)?				
А.6.2 Внешние организационные аспекты ***Организация должна:***				
Обеспечить безопасность информации и средств обработки информации организации, которые доступны, обрабатываются, известны или управляются сторонними организациями.				
А.6.2.1 Были ли идентифицированы риски для информации и средств обработки информации организации, возникающие в бизнес-процессах, в которые вовлечены внешние организации, и были ли реализованы надлежащие средства управления до того, как к этой информации и средствам был предоставлен доступ?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.6.2.2 Были ли учтены все идентифицированные требования безопасности перед предоставлением заказчикам доступа к информации или ресурсам организации?				
А.6.2.3 Учитываются ли все необходимые требования безопасности в соглашениях со сторонними организациями, которые предусматривают доступ, обработку, использование, управление информацией или средствами обработки информации организации либо добавление продуктов или сервисов в средства обработки информации?				
А.7 Управление ресурсами				
А.7.1 Ответственность за ресурсы ***Организация должна:***				
Обеспечить и поддерживать надлежащую защиту ресурсов организации.				
А.7.1.1 Были ли все ресурсы явно идентифицированы, была ли составлена и поддерживается ли в актуальном состоянии опись всех важных ресурсов?				
А.7.1.2 Находятся ли вся информация и ресурсы, связанные со средствами обработки информации, «во владении» [1] уполномоченного подразделения организации?				
А.7.1.3 Были ли идентифицированы, документированы и реализованы правила допустимого использования информации и ресурсов, связанных со средствами обработки информации?				
А.7.2 Классификация информации ***Организация должна:***				
Гарантировать, что обеспечен надлежащий уровень защиты информации.				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.7.2.1 Классифицирована ли информация по таким показателям, как значимость, правовые требования, чувствительность к воздействиям и критичность для организации?				
А.7.2.2 Был ли разработан и реализован в соответствии с принятой в организации системой классификации надлежащий набор процедур для маркировки и обращения с информацией?				
А.8 Аспекты безопасности, связанные с персоналом				
А.8.1 До найма на работу ***Организация должна:***				
Гарантировать, что сотрудники, подрядчики и пользователи из сторонних организаций понимают свою ответственность и подходят для предназначаемых им ролей, а также уменьшить риск кражи, мошенничества или неправильного использования оборудования.				
А.8.1.1 Производится ли определение и документирование ролей безопасности и ответственности сотрудников, подрядчиков и пользователей из сторонних организаций в соответствии с политикой информационной безопасности организации?				
А.8.1.2 Выполняются ли проверки персональных данных всех кандидатов на вакансии, подрядчиков и пользователей из сторонних организаций согласно соответствующим законам, нормативным документам и этическим нормам, а также с учетом бизнес-требований, категории информации, к которой будет предоставлен доступ, и осознаваемым рискам?				
А.8.1.3 Входит ли в контрактные обязательства сотрудников, подрядчиков и пользователей из сторонних организаций обязательство принимать и подписывать положения и условия своего контракта о найме, и установлена ли в этом контракте их				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
ответственность и ответственность организации за информационную безопасность?				
А.8.2 Во время найма ***Организация должна:***				
Гарантировать, что сотрудники, подрядчики и пользователи из сторонних организаций осведомлены об угрозах информационной безопасности и ее значении, о своей ответственности и обязательствах, способны поддерживать политику безопасности организации в процессе своей обычной работы, а также уменьшить риск субъективных ошибок.				
А.8.2.1 Требует ли руководство, чтобы сотрудники, подрядчики и пользователи из сторонних организаций применяли правила информационной безопасности в соответствии с установленными в организации политиками и процедурами?				
А.8.2.2 Получают ли все сотрудники организации и, где необходимо, подрядчики и пользователи из сторонних организаций надлежащее осведомляющее обучение и информацию об обновлениях политик и процедур организации, в объеме, необходимом для выполнения ими своих рабочих функций?				
А.8.2.3 Определен ли формальный дисциплинарный процесс для сотрудников, которые нарушили безопасность?				
А.8.3 Увольнение или изменение условий найма ***Организация должна:***				
Гарантировать, что сотрудники, подрядчики и пользователи из сторонних организаций покидают организацию или изменяют условия найма в установленном порядке.				
А.8.3.1 Была ли определена и назначена ответственность за выполнение процедур увольнения сотрудников или изменения условий найма?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.8.3.2 Обязаны ли все сотрудники, подрядчики и пользователи из сторонних организаций вернуть все ресурсы организации, находившиеся в их распоряжении, при увольнении или окончания срока действия контракта (соглашения)?				
А.8.3.3 Производится ли аннулирование прав доступа всех сотрудников, подрядчиков и пользователей из сторонних организаций к информации и средствам обработки информации в случае увольнения, прекращения контракта или соглашения, и изменяются ли указанные права доступа в случае изменения условий найма?				
А.9 Физическая безопасность и безопасность среды функционирования				
А.9.1 Защищенные области ***Организация должна:***				
Предотвратить несанкционированный физический доступ, ущерб или влияние на территорию, оборудование и информацию организации.				
А.9.1.1 Используются ли периметры безопасности (барьеры, такие как стены, вход, оборудованный системой пропуска по картам, или контроль входящих специальным персоналом) для защиты областей, в которых находится информация и средства обработки информации?				
А.9.1.2 Защищены ли защищаемые области необходимыми средствами контроля доступа в помещения, позволяющими обеспечить доступ к ним только персонала, получившего соответствующие полномочия?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.9.1.3 Были ли разработаны и внедрены меры физической безопасности для защиты офисов, комнат и оборудования?				
А.9.1.4 Были ли разработаны и внедрены меры физической защиты от пожара, затопления, землетрясения, взрыва, гражданских беспорядков и других форм природных и антропогенных катастроф?				
А.9.1.5 Были ли разработаны и внедрены меры физической защиты и инструкции по работе в защищенных областях?				
А.9.1.6 Осуществляется ли контроль мест свободного доступа, таких как площадки для разгрузки и погрузки и другие места, куда возможен доступ неуполномоченных лиц, и изолируются ли, при возможности, указанные места от средств обработки информации в целях предотвращения несанкционированного доступа?				
А.9.2 Защита оборудования ***Организация должна:***				
Предотвратить потерю, повреждение, кражу или компрометацию ресурсов, а также перебои в деятельности организации.				
А.9.2.1 Осуществляется ли размещение или защита оборудования так, чтобы уменьшить риски и ущерб, связанные с воздействием внешней среды, а также вероятность несанкционированного доступа?				
А.9.2.2 Защищено ли оборудование от сбоев в системе электропитания и других неполадок, возникающих из-за сбоев в поддерживающей инфраструктуре?				
А.9.2.3 Защищены ли кабельные системы электропитания и телекоммуникаций, используемые для передачи данных или поддержки информационных сервисов, от прослушивания или повреждения?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.9.2.4 Обеспечивается ли надлежащее сопровождение оборудования, позволяющее гарантировать его постоянную доступность и целостность?				
А.9.2.5 Применяются ли к оборудованию за пределами организации меры безопасности, учитывающие различные риски работы вне территории организации?				
А.9.2.6 Проверяются ли перед утилизацией все единицы оборудования, содержащие носители информации, чтобы гарантировать, что все критичные данные и лицензионное программное обеспечение были удалены с них или надежно замещены другой информацией?				
А.9.2.7 Требуется ли санкция руководства на вынос оборудования, информации или программного обеспечения за пределы организации?				
А.10 Управление коммуникациями и функционированием				
А.10.1 Операционные процедуры и ответственность ***Организация должна:***				
Обеспечить корректное и защищенное функционирование средств обработки информации.				
А.10.1.1 Задокументированы ли операционные процедуры, обеспечено ли их сопровождение, а также доступность для всех пользователей, которым они требуются?				
А.10.1.2 Контролируются ли изменения в средствах и системах обработки информации?				
А.10.1.3 Разделены ли обязанности и зоны ответственности для уменьшения вероятности несанкционированной или непреднамеренной модификации или ненадлежащего использования ресурсов организации?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
A.10.1.4 Разделены ли средства разработки, тестирования и производственные средства для уменьшения рисков несанкционированного доступа или изменений операционной системы?				
A.10.2 Управление предоставлением сервисов сторонних организаций ***Организация должна:***				
Реализовать и поддерживать надлежащий уровень информационной безопасности и предоставления сервисов в соответствии с соглашением о поставке сервисов сторонней организацией.				
A.10.2.1 Разработаны ли процедуры, позволяющие гарантировать, что средства управления безопасностью, определения сервисов и уровни поставки, включенные в соглашение о поставке сервисов сторонней организацией, реализованы, функционируют и сопровождаются сторонней организацией?				
A.10.2.2 Подвергаются ли регулярному мониторингу и анализу сервисы, отчеты и записи, предоставляемые сторонней организацией, и регулярно ли проводятся аудиты?				
A.10.2.3 Осуществляется ли управление изменениями в предоставлении сервисов, включая сопровождение и совершенствование существующих политик информационной безопасности, процедур и средств управления, и учитывается ли при этом критичность вовлеченных бизнес-систем и процессов, а также повторная оценка рисков?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	**ЧАСТИЧНО (выполняется частично)**	**НЕТ (не выполняется)**	
А.10.3 Планирование систем и их приемка ***Организация должна:***				
Минимизировать риск отказов систем.				
А.10.3.1 Проводится ли мониторинг и оптимизация использования ресурсов, составляются ли прогнозы будущих потребностей с целью обеспечить необходимую производительность системы?				
А.10.3.2 Установлены ли критерии приемки новых информационных систем, модернизаций и новых версий, и выполняется ли надлежащее тестирование системы во время ее разработки, но до приемки системы?				
А.10.4 Защита от вредоносного и мобильного программного кода ***Организация должна:***				
Обеспечить целостность программного обеспечения и информации.				
А.10.4.1 Реализованы ли средства обнаружения, предотвращения и восстановления, обеспечивающие защиту от вредоносного программного кода, а также надлежащие процедуры оповещения пользователей?				
А.10.4.2 Гарантирует ли используемая конфигурация, что там, где разрешено использование мобильного кода, санкционированный мобильный код функционирует в соответствии с явно заданной политикой безопасности, а исполнение несанкционированного мобильного кода не допускается?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.10.5 Резервное копирование ***Организация должна:***				
Обеспечить целостность и доступность информации и средств обработки информации.				
А.10.5.1 Выполняется ли регулярное создание и тестирование резервных копии информации и программного обеспечения в соответствии с установленной политикой резервного копирования?				
А.10.6 Управление безопасностью сетей ***Организация должна:***				
Обеспечить защиту информации в сетях и защиту поддерживающей инфраструктуры.				
А.10.6.1 Осуществляется ли надлежащее управление и контроль сетей с целью защиты от угроз и для поддержки безопасности систем и приложений, использующих сеть, включая информацию, передаваемую по сетям?				
А.10.6.2 Идентифицированы ли требования к средствам безопасности, уровню сервисов и требования по управлению для всех сетевых сервисов и включены ли эти требования во все соглашения относительно сетевых сервисов, не того, предоставляются ли эти сервисы силами самой и или внешними организациями (аутсорсинг)?				
А.10.7 Управление носителями информации и их защита ***Организация должна:***				
Предотвратить повреждение информационных ресурсов и приостановку работы организации.				
А.10.7.1 Установлены ли процедуры управления съемными носителями информации?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.10.7.2 Уничтожаются ли безопасным и надежным способом, с соблюдением формальных процедур, носители информации, которые больше не нужны?				
А.10.7.3 Установлены ли процедуры обращения с информацией и хранения информации, предназначенные для защиты информации от несанкционированного раскрытия или ненадлежащего использования?				
А.10.7.4 Осуществляется ли защита системной документации от несанкционированного доступа?				
А.10.8 Обмен информацией ***Организация должна:***				
Обеспечить безопасность информации и программного обеспечения, которые являются предметом информационного обмена как внутри организации, так и с любыми внешними объектами.				
А.10.8.1 Установлены ли формальные политики и процедуры обмена, а также средства управления обменом, предназначенные для защиты обмена информацией с использованием средств коммуникации всех типов?				
А.10.8.2 Были ли заключены соглашения об обмене информацией и программным обеспечением между организацией и внешними организациями?				
А10.8.3 Защищаются ли от несанкционированного доступа, ненадлежащего использования или повреждения содержащие информацию носители во время их транспортировки за пределами территории организации?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.10.8.4 Защищается ли надлежащим образом информация, циркулирующая в системах обмена электронными сообщениями?				
А.10.8.5 Были ли разработаны и реализованы политики и процедуры для защиты информации, связанной с объединением информационных систем бизнеса?				
А.10.9 Сервисы электронной коммерции ***Организация должна:***				
Обеспечить безопасность сервисов электронной коммерции, а также их безопасное использование **.**				
А.10.9.1 Защищается ли информация, используемая в электронной коммерции и проходящая через общедоступные сети, от мошеннических действий, споров по контрактам, несанкционированного разглашения и модификации?				
А.10.9.2 Осуществляется ли защита информации, используемой в операциях он-лайн (выполняемых в реальном времени), с целью предотвратить неполную передачу, неверную маршрутизацию, несанкционированную замену сообщений, несанкционированное разглашение, несанкционированное дублирование или воспроизведение сообщений?				
А.10.9.3 Защищается ли целостность информации, циркулирующей в общедоступных системах, от несанкционированной модификации?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.10.10 Мониторинг ***Организация должна:***				
Обнаружить несанкционированные действия по обработке информации.				
А.10.10.1 Осуществляется ли ведение и хранение в течение установленного периода журналов аудита, регистрирующих действия пользователей, исключительные ситуации и события информационной безопасности, с целью использования этих журналов в будущих обследованиях и при мониторинге управления доступом?				
А.10.10.2 Были ли установлены процедуры мониторинга использования средств обработки информации, и проводится ли регулярный анализ результатов мониторинга?				
А.10.10.3 Защищаются ли средства ведения журналов и информация журналов от тайных воздействий и несанкционированного доступа?				
А.10.10.4 Регистрируются ли действия системного администратора и оператора системы в соответствующих журналах?				
А.10.10.5 Осуществляется ли регистрация сбоев в журнале, проводится ли их анализ, и принимаются ли соответствующие меры?				
А.10.10.6 Синхронизируются ли часы всех важных систем обработки информации в рамках организации или домена безопасности по установленному источнику точного времени?				
А.11 Управление доступом				
А.11.1 Бизнес-требования к управлению доступом ***Организация должна:***				
Управлять доступом к информации.				
А.11.1.1 Была ли установлена и документирована политика				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
управления доступом, основанная на требованиях к доступу со стороны бизнеса и безопасности, и осуществляется ли регулярный пересмотр этой политики?				
А.11.2 Управление доступом пользователей ***Организация должна:***				
Обеспечить санкционированный доступ пользователей и предотвратить несанкционированный доступ к информационным системам.				
А.11.2.1 Установлена ли формальная процедура регистрации и отмены регистрации пользователей для предоставления и аннулирования доступа ко всем информационным системам и сервисам?				
А.11.2.2 Является ли предоставление и использование полномочий ограниченным и контролируемым?				
А.11.2.3 Контролируется ли назначение паролей посредством формального процесса управления?				
А.11.2.4 Пересматривает ли руководство права доступа пользователей через регулярные интервалы времени, используя формальный процесс?				
А.11.3 Ответственность пользователей ***Организация должна:***				
Предотвратить несанкционированный доступ пользователей, а также компрометацию или кражу информации и средств обработки информации.				
А.11.3.1 Обязаны ли пользователи при выборе и использовании паролей придерживаться принципов безопасности, на практике доказавших свою эффективность?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.11.3.2 Обязаны ли пользователи обеспечивать надлежащую защиту оборудования, оставляемого без присмотра?				
А.11.3.3 Была ли принята политика «чистый стол» для бумаг и съемных носителей информации и политика «чистый экран» для средств обработки информации?				
А.11.4 Управление доступом к сети ***Организация должна:***				
Предотвратить несанкционированный доступ к сетевым сервисам.				
А.11.4.1 Предоставляется ли пользователям доступ только к тем сервисам, использование которых им явным образом разрешено?				
А.11.4.2 Используются ли надлежащие методы аутентификации для контроля доступа удаленных пользователей?				
А.11.4.3 Была ли учтена автоматическая идентификация оборудования в качестве средства аутентификации соединений, устанавливаемых конкретными узлами и оборудованием?				
А.11.4.4 Контролируется ли физический и логический доступ к диагностическим и конфигурационным портам?				
А.11.4.5 Установлены ли в сетях средства управления, позволяющие разделить (изолировать) группы информационных сервисов, пользователей и информационных систем?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.11.4.6 Ограничиваются ли для коллективно используемых сетей (особенно для тех, которые выходят за пределы организации) возможности пользователей по подключению к сети, и соответствует ли применение этих ограничений политике управления доступом и требованиям бизнес-приложений (см. А.11.1)?				
А.11.4.7 Были ли реализованы в сетях средства управления маршрутизацией, позволяющие гарантировать, что подключения компьютерных систем и информационные потоки не нарушают политику управления доступом для бизнес-приложений?				
А.11.5 Контроль доступа к операционной системе ***Организация должна:***				
Предотвратить несанкционированный доступ к операционным системам.				
А.11.5.1 Контролируется ли доступ к операционным системам с помощью безопасной процедуры входа в систему?				
А.11.5.2 Предоставляется ли всем пользователя уникальный идентификатор (ИД пользователя) только для личного использования, и был ли выбран подходящий метод аутентификации, позволяющий подтверждать заявленную личность пользователя?				
А.11.5.3 Являются ли системы управления паролями интерактивными, и обеспечивают ли эти системы качественные пароли?				
А.11.5.4 Является ли ограниченным и строго контролируемым использование системных программ-утилит, с помощью которых можно изменить систему и средства управления приложениями?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.11.5.5 Используются ли средства управления, позволяющие закрывать неактивные сеансы по истечении заданного времени бездействия?				
А.11.5.6 Используются ли ограничения по времени подключения для обеспечения дополнительной защиты приложений высокого риска?				
А.11.6 Управление доступом к приложениям и их информации ***Организация должна:***				
Предотвратить несанкционированный доступ к информации, хранимой в прикладных системах.				
А.11.6.1 Ограничивается ли доступ пользователей и обслуживающего персонала к информации и функциям прикладных систем в соответствии с заданной политикой управления доступом?				
А.11.6.2 Обеспечивается ли для функционирования критичных систем выделенная (изолированная) вычислительная среда?				
А.11.7 Мобильные вычисления и дистанционная работа. ***Организация должна:***				
Обеспечить информационную безопасность при использовании средств мобильных вычислений и дистанционной работы.				
А.11.7.1 Существует ли формальная политика и были ли приняты надлежащие меры безопасности, позволяющие обеспечить защиту от рисков, связанных с использованием средств мобильных вычислений и коммуникации?				
А.11.7.2 Были ли разработаны и реализованы политика, оперативные планы и процедуры для дистанционной работы?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.12 Приобретение, разработка и сопровождение информационных систем				
А.12.1 Требования к безопасности информационных систем ***Организация должна:***				
Гарантировать, что безопасность является компонентом информационных систем.				
А.12.1.1 Устанавливают ли формулировки бизнес-требований к новым информационным системам или к модернизации существующих информационных систем требования к средствам управления безопасностью?				
А.12.2 Корректная обработка в приложениях ***Организация должна:***				
Предотвратить ошибки, потерю, несанкционированную модификацию или ненадлежащее использование информации в приложениях.				
А.12.2.1 Производится ли проверка достоверности входных данных приложений, чтобы гарантировать, что эти данные являются корректными и правильными?				
А.12.2.2 Встроены ли в приложения проверки достоверности, позволяющие выявлять любые повреждения информации из-за ошибок обработки или умышленных действий?				
А.12.2.3 Были ли идентифицированы требования к обеспечению аутентичности и защите целостности сообщений в приложениях, и были ли идентифицированы и реализованы соответствующие средства управления?				
А.12.2.4 Выполняется ли проверка выходных данных приложения на достоверность, чтобы гарантировать, что обработка хранимой информации корректна и соответствует текущим обстоятельствам?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.12.3 Криптографические средства управления ***Организация должна:***				
Обеспечить защиту конфиденциальности, аутентичности и целостности информации криптографическими средствами.				
А.12.3.1 Была ли разработана и реализована политика использования криптографических средств управления для защиты информации?				
А.12.3.2 Реализовано ли управление ключами, позволяющее поддерживать в организации использование криптографических методов?				
А.12.4 Безопасность системных файлов ***Организация должна:***				
Обеспечить безопасность системных файлов.				
А.12.4.1 Разработаны ли процедуры контроля установки программного обеспечения в действующих системах?				
А.12.4.2 Осуществляется ли тщательный выбор тестовых данных, их защита и контроль?				
А.12.4.3 Ограничивается ли доступ к исходному коду программ?				
А.12.5 Безопасность процессов разработки и технического обслуживания ***Организация должна:***				
Поддерживать безопасность программного обеспечения и информации прикладных систем.				
А.12.5.1 Используются ли для контроля реализации изменений формальные процедуры управления изменениями?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.12.5.2 Проводится ли при изменении действующих систем анализ и тестирование критичных для бизнеса приложений, чтобы гарантировать отсутствие неблагоприятного воздействия на функционирование и безопасность организации?				
А.12.5.3 Ограничиваются ли модификации пакетов программного обеспечения, производятся ли только необходимые изменения, и осуществляется ли строгий контроль всех изменений?				
А.12.5.4 Предотвращаются ли возможности для утечки информации				
А.12.5.5 Осуществляет ли организация контроль и отслеживание разработки программного обеспечения сторонними организациями (аутсорсинг)?				
А.12.6 Управление техническими уязвимостями ***Организация должна:***				
Уменьшить риски, возникающие из-за использования опубликованных данных о технических уязвимостях.				
А.12.6.1 Своевременно ли получает организация информацию о технических уязвимостях используемых информационных систем, оценивается ли незащищенность организации перед этими уязвимостями, и принимаются ли адекватные меры для устранения рисков, связанных с такими уязвимостями?				
А.13 Управление инцидентами информационной безопасности				
А.13.1 Составление отчетов о событиях информационной безопасности и слабостях защиты ***Организация должна:***				
Гарантировать, что о событиях информационной безопасности и слабостях защиты, связанных с информационными системами, сообщается таким образом, что это позволяет своевременно принимать корректирующие меры.				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.13.1.1 Осуществляется ли оповещение о событиях информационной безопасности по надлежащим управленческим каналам настолько быстро, насколько это возможно?				
А.13.1.2 Обязаны ли все сотрудники, подрядчики и пользователи из сторонних организаций, использующие информационные системы и сервисы, отмечать и сообщать обо всех наблюдаемых или предполагаемых слабостях защиты систем или сервисов?				
А.13.2 Управление инцидентами и совершенствованием информационной безопасности ***Организация должна:***				
Гарантировать, что применяется непротиворечивый и эффективный подход к управлению инцидентами информационной безопасности.				
А.13.2.1 Установлены ли ответственность руководства и процедуры, обеспечивающие быстрое, эффективное и правильное реагирование на инциденты информационной безопасности?				
А.13.2.2 Реализованы ли механизмы, позволяющие измерять и отслеживать типы, объемы и стоимость инцидентов информационной безопасности?				
А.13.2.3 Если действия, которые в результате инцидента информационной безопасности предполагается предпринять относительно лица или организации, включают в себя правовые действия (как по гражданскому, так и по уголовному кодексу), то осуществляется ли сбор, сохранение и представление доказательства в соответствии с правилами доказательства, установленными в соответствующем правоохранительном органе (органах)?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.14 Управление непрерывностью бизнеса				
А.14.1 Аспекты информационной безопасности в управлении непрерывностью бизнеса ***Организация должна*:**				
Противодействовать перебоям в бизнес-деятельности и обеспечить защиту критичных бизнес-процессов от последствий крупных аварий информационных систем или катастроф, а также обеспечить своевременное восстановление работы.				
А.14.1.1 Был ли разработан и поддерживается ли управляемый процесс обеспечения непрерывности бизнеса в рамках организации, который учитывает требования информационной безопасности, необходимые для непрерывности бизнеса данной организации?				
А.14.1.2 Идентифицированы ли все события, из-за которых возможны остановки бизнес-процессов, и определены ли вероятность и воздействие таких остановок и их влияние на информационную безопасность?				
А.14.1.3 Были ли разработаны и реализованы планы, позволяющие поддерживать или восстанавливать операции, а также обеспечивать на требуемом уровне и за требуемое время доступность информации после остановки или сбоя критичных бизнес-процесссов?				
А.14.1.4 Поддерживается ли единая структура планов обеспечения непрерывности бизнеса, позволяющая гарантировать непротиворечивость всех планов, постоянный учет требований информационной безопасности и определение приоритетов для тестирования и сопровождения?				
А.14.1.5 Проводится ли регулярное тестирование и обновление планов обеспечения непрерывности бизнеса, чтобы гарантировать их актуальность и эффективность?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.15 Соответствие формальным требованиям				
А.15.1 Соответствие правовым требованиям ***Организация должна:***				
Избежать нарушений законов, основанных на законе обязательств, регулятивных или договорных обязательств, а также всех требований безопасности.				
А.15.1.1 Были ли для каждой информационной системы и организации явно определены, документированы и поддерживаются ли в актуальном состоянии все требования закона, регулятивные и договорные требования, а также подход организации, используемый для удовлетворения этих требований?				
А.15.1.2 Реализованы ли надлежащие процедуры, гарантирующие соответствие правовым, регулятивным и договорным требованиям по использованию материалов, на которые могут распространяться права на интеллектуальную собственность, а также по использованию патентованных программных продуктов?				
А.15.1.3 Осуществляется ли защита важных записей от потери, уничтожения и подделки в соответствии с требованиями закона, регулятивными и договорными требованиями, а также бизнес-требованиями?				
А.15.1.4 Применяются ли средства управления, обеспечивающие защиту и конфиденциальность данных, в соответствии с требованиями соответствующего законодательства, регулятивных положений и, в случае применимости, положений договоров?				

Проверяемое требование стандарта	Оценка выполнения требования стандарта			Рекомендации по выполнению требования стандарта
	ДА (выполняется полностью)	ЧАСТИЧНО (выполняется частично)	НЕТ (не выполняется)	
А.15.1.5 Принимаются ли меры, удерживающие пользователей от использования средств обработки информации для несанкционированных целей?				
А.15.1.6 Соответствует ли использование криптографических средств управления всем релевантным соглашениям, законам и регулятивным положениям?				
А.15.2 Соответствие политикам безопасности и стандартам, техническое соответствие ***Организация должна:***				
Обеспечить соответствие систем принятым в организации политикам и стандартам безопасности.				
А.15.2.1 Принимают ли менеджеры меры для обеспечения корректного выполнения всех процедур безопасности в их сфере ответственности, чтобы гарантировать соответствие политикам и стандартам безопасности?				
А.15.2.2 Выполняется ли регулярная проверка информационных систем на соответствие стандартам обеспечения безопасности?				
А.15.3 Анализ аудита информационных систем ***Организация должна:***				
Максимизировать эффективность процесса аудита и минимизировать воздействие, с одной стороны, процесса аудита на информационные системы, а с другой – информационных систем на процесс аудита.				
А.15.3.1 Выполняется ли тщательное планирование и согласование требований аудита и деятельности, включающей проверки производственных систем, чтобы минимизировать риск сбоев в бизнес-процессах?				
А.15.3.2 Осуществляется ли защита доступа к средствам аудита информационных систем с целью предотвратить любое возможное ненадлежащее использование или компрометацию?				

6 Аудит целей и средств управления, предусмотренных стандартом *СТ РК ИСО/МЭК 27001*

6.1 Политика безопасности

6.1.1 Политика информационной безопасности

Цель: Сформулировать цель и обеспечить поддержку информационной безопасности руководством организации.

6.1.1.1 Документ о политике информационной безопасности

Письменный документ о политике информационной безопасности должен быть утвержден руководством организации, опубликован и доведен до сведения всех сотрудников.

Руководство по аудиту:

Данная политика не должна вдаваться в излишние детали, однако в ней должно быть четко зафиксировано стремление руководства обеспечить информационную безопасность, по ней должен вестись учет изменений, а на документе должна присутствовать подпись ответственного руководящего лица. Политика должна включать в себя, как минимум, следующие сведения:

– Определение информационной безопасности,

– Причины, по которым информационная безопасность важна для организации; принципы и цели информационной безопасности,

– Краткие сведения о политиках безопасности, принципах, стандартах и требованиях на соответствие,

– Определение всех релевантных обязанностей по обеспечению информационной безопасности,

– Ссылки на соответствующие дополнительные документы.

Аудитору следует убедиться в том, что политика легко доступна любому из сотрудников, все сотрудники осведомлены о ее существовании и понимают ее смысл. Политика может представлять собой отдельный документ либо входить в состав более подробного документа (например, руководства по политике безопасности), определяющего, каким образом политика информационной безопасности внедряется в организации. Чаще всего большинство, если не все сотрудники, подпадающие под область применения СУИБ, имеют определенные обязанности в сфере информационной безопасности, и аудиторам следует обращать внимание на любые заявления, отрицающие этот факт.

Кроме того, аудитор должен убедиться в том, что определено лицо, ответственное за поддержание политики, а сама политика обновляется в соответствии с любыми изменениями, затрагивающими аспекты, на основе которых проводилась оценка рисков.

6.1.1.2 Пересмотр и анализ

Политика должна регулярно и в случае значимых изменений анализироваться и пересматриваться с целью сохранения ее адекватности.

Руководство по аудиту:

Данное средство управления необходимо для обеспечения актуальности и эффективности политики информационной безопасности. Эта политика играет важную роль при создании и поддержке СУИБ. Аудиторам необходимо убедиться, что в организации разработаны процедуры реагирования на любые инциденты, новые уязвимости и угрозы безопасности, технологические изменения и все остальное, что имеет отношение к СУИБ и может потребовать переоценки политики. Кроме того, в организации должен быть запланирован периодический пересмотр политики с целью удостовериться, что политика актуальна и её внедрение экономически оправданно по отношению к уровню предоставляемой защиты. Аудитору необходимо убедиться в том, что график пересмотра политики соответствует общей ситуации по рискам. Аудиторы также должны проверить планы организации по распространению обновленных версий политики и убедиться, что информация о внесенных изменениях доводится до всех сотрудников.

6.2 Обеспечение безопасности

6.2.1 Инфраструктура информационной безопасности

Цель: Управлять информационной безопасностью в организации.

Для утверждения политики информационной безопасности, распределения обязанностей по обеспечению безопасности и координации внедрения безопасности в пределах организации должны быть проведены соответствующие совещания с высшим руководством. При необходимости следует предусмотреть способы получения сведений и советов по информационной безопасности у специалистов и обеспечить доступ к этим сведениям в пределах организации. Следует наладить и поддерживать контакты с внешними специалистами по безопасности для отслеживания текущих тенденций, стандартов и методов оценки в данной области, а также для выработки надлежащих способов связи со специалистами при работе с инцидентами безопасности. Необходимо поощрять междисциплинарный подход к информационной безопасности, например, сотрудничество менеджеров, пользователей, администраторов, разработчиков приложений, аудиторов и специалистов по безопасности в таких областях, как страхование и управление рисками.

6.2.1.1 Совещание руководства по проблемам защиты информации и координация действий по защите информации

Руководство организации должно регулярно проводить совещания для выработки четких указаний и обеспечения административной поддержки инициативам по обеспечению безопасности. Совещания руководства должны

способствовать обеспечению безопасности посредством необходимого участия и выделения достаточных ресурсов.

В крупных организациях должны проводиться совещания с участием руководителей различных подразделений с целью координации действий по реализации средств управления информационной безопасностью.

Руководство по аудиту:

Это механизм, необходимый для идентификации потребностей организации в области безопасности, а также для обеспечения их адекватного удовлетворения и периодического пересмотра. Предполагается, что эта группа будет ответственна за создание и поддержку СУИБ. Участники совещания должны обладать соответствующими полномочиями, поэтому аудиторам следует убедиться, что оно проводится под руководством, или как минимум при участии, лица, ответственного за информационную безопасность. Протокол заседаний должен фиксироваться формально; любые действия, о проведении которых было принято решение, должны отслеживаться с помощью четко определенной процедуры. Необходим прагматический подход к проведению совещания; для небольших организаций может оказаться целесообразным совместить проведение совещания по информационной безопасности с другими мероприятиями, однако в этом случае необходимо обеспечить адекватное освещение вопросов информационной безопасности и проследить, чтобы в протоколе были четко зафиксированы проблемы, касающиеся безопасности.

Крупные организации, а также организации с повышенными требованиями к информационной безопасности должны посвятить обсуждению вопросов безопасности отдельное совещание. Аудитору необходимо убедиться в том, что эти совещания, а также прочие мероприятия, такие как пересмотр политики безопасности, проводятся с достаточной периодичностью. Число и состав участников совещания определяются требованиями конкретной организации. Например, в небольшой организации в совещании могут участвовать только исполнительный директор и ответственный за информационную безопасность, а для крупных концернов уместен формат расширенного совещания с участием высшего руководства, представителей каждого подразделения и сотрудников по безопасности. Аудитор должен оценивать каждую ситуацию, исходя из потребностей конкретной организации и заявленного масштаба СУИБ. Учитывая современные темпы развития технологий, организация, использующая средства обработки информации, должна пересматривать процедуры по обеспечению безопасности как минимум раз в шесть месяцев.

6.2.1.2 Распределение обязанностей по обеспечению информационной безопасности

Должны быть четко определены обязанности по защите отдельных ресурсов и по выполнению конкретных процессов обеспечения безопасности.

Руководство по аудиту:

Аудиторам необходимо убедиться в том, что обязанности на всех уровнях четко определены. Осведомленность об обязанностях и принятие персоналом ответственности должны быть подтверждены соответствующими свидетельствами. Для определения ответственности и состава отчетности на более высоком уровне обычно используется политика безопасности и/или план обработки рисков, однако конкретные аспекты ответственности за информационную безопасность чаще всего включаются в описание должностных обязанностей либо указываются в ином формате, в зависимости от конкретной ситуации. Необходимо, чтобы по каждому ресурсу было определено лицо, ответственное за обеспечение его безопасности. Аудиторам следует убедиться, что в организации назначено лицо, ответственное за информационную безопасность в целом (например, руководитель по информационной безопасности), и все ответственные сотрудники осведомлены о своих обязанностях по обеспечению информационной безопасности. Аудиторы также должны проверить, что вся соответствующая документация актуальна на текущий момент и ее обновление надлежащим образом контролируется.

6.2.1.3 Процесс утверждения информационных систем

Должна быть определена процедура утверждения руководством новых информационных систем.

Руководство по аудиту:

Крайне важно соблюдать целостность средств управления безопасностью. Соответственно, расширение либо изменение набора информационных систем должно надлежащим образом контролироваться со стороны руководства. Процедуры утверждения и получения разрешения должны быть четко сформулированы и реализованы, а также подтверждены соответствующей документацией. Аудиторам необходимо убедиться в том, что установка новых программных средств, обновление версий, изменение настроек, а также любые другие процедуры, затрагивающие инфраструктуру безопасности, одобрены руководством организации на соответствующем уровне, проверены с технической точки зрения, отслеживаются в плане изменения настроек и должным образом документируются. Ввод новых систем и использование их сотрудниками в производственных целях должны быть разрешены руководством явным образом.

6.2.1.4 Рекомендации специалистов по информационной безопасности

Организация должна обращаться за рекомендациями по обеспечению информационной информации к собственным или внешним консультантам и

обязана координировать реализацию полученных рекомендаций в рамках всей организации.

Руководство по аудиту:

Вопрос, когда и в каких объемах прибегать к консультациям по вопросам информационной безопасности, целиком относится к компетенции конкретной организации. В одном случае целесообразно привлечь консультантов или другой источник сведений по информационной безопасности внутри организации, в другом – прибегнуть к помощи сторонних специалистов или организаций, таких как профессиональные консультанты или признанные эксперты в данной области, а в третьем – использовать комбинированный подход. Независимо от выбранного подхода должна поддерживаться четкая связь с совещаниями по безопасности. Аудитору следует определить, какие дополнительные сведения предоставляются, адекватны ли они ситуации, достаточно ли квалифицирован источник информации, а также выявить области, где явно требуются консультации, однако запроса на них не поступало. При этом доступ к средствам управления безопасностью должен быть надлежащим образом авторизован руководством, а при необходимости дополнительно проконтролирован поставщиком оборудования. Рекомендуется также проанализировать отчеты по инцидентам безопасности: принимали ли назначенные специалисты участие в оценке причин инцидента, проводились ли рекомендованные коррекционные мероприятия? В небольших организациях ответственный специалист по безопасности (или сотрудник, занимающий эквивалентную должность) может оказаться единственным источником сведений по информационной безопасности. В этом случае аудиторам необходимо удостовериться в том, что этого достаточно для удовлетворения имеющихся требований по безопасности, что в организации отслеживаются изменения в области технологий и безопасности и что при необходимости для консультаций привлекаются внешние ресурсы.

6.2.1.5 Сотрудничество между организациями

Должны поддерживаться необходимые контакты с правоохранительными органами, контролирующими органами, поставщиками информационных услуг и операторами услуг связи.

Руководство по аудиту:

Данное средство управления требует наличия каналов связи с внешними контролирующими органами, поставщиками услуг и другими организациями, которые могут играть существенную роль при предотвращении инцидентов безопасности или минимизации их последствий. Соответственно, аудитор должен определить наличие нужных контактных лиц, занимающихся планированием действий в чрезвычайных обстоятельствах и поддержкой инфраструктуры. Аудитору необходимо найти свидетельства того, что в организации следят за требованиями в

правовой сфере, а также за операционными и техническим требованиями производственного плана, и обеспечивают соответствие этим требованиям. Аудитору следует убедиться в том, что организации известны все применимые к ситуации законодательные требования, что эти требования документированы и налажены все контакты, необходимые для выполнения требований.

Кроме того, организации полезно принимать участие в распространении передовых практик и обмениваться информацией о распространенных угрозах в своей отрасли. Крупные организации могут участвовать в работе специализированных групп по безопасности, комитетов по принятию стандартов и в прочих внепроизводственных мероприятиях подобного рода. Небольшие организации обычно не имеют возможности принимать активное участие в таких мероприятиях, однако посещение профильных конференций и семинаров может частично компенсировать этот факт.

6.2.1.6 Независимый анализ информационной безопасности

Должен проводиться независимый анализ реализации политики информационной безопасности.

Руководство по аудиту:

Аудитор должен убедиться в том, что периодический анализ действительно проводится и выполняется независимыми лицами. Без проведения независимого анализа невозможно гарантировать полную объективность. Аудит, выполняемый сторонними специалистами, удовлетворяет описанным выше требованиям. В случаях, когда сторонний аудит не проводится, возможно проведение анализа внутренними аудиторами, руководством или другими лицами, работающими отдельно от сотрудников, обеспечивающих информационную безопасность. Необходимо также учитывать результаты прочих проверок, таких как проверка безопасности информационных систем (см. 6.10.2).

6.2.2 Безопасность доступа сторонних организаций

Цель: Обеспечить безопасность информационных ресурсов организации, к которым имеют доступ сторонние организации.

6.2.2.1 Идентификация рисков, связанных с доступом сторонних организаций

Должна быть выполнена оценка рисков, связанных с доступом сторонних организаций к информационным ресурсам организации, и должны быть реализованы соответствующие средства управления безопасностью.

Руководство по аудиту:

В первую очередь аудитору необходимо проверить оценку, выполненную организацией для выявления рисков, связанных с доступом третьих учреждений/лиц к информационным ресурсам. Риски могут быть связаны с удаленным доступом к вычислительному узлу или серверному программному обеспечению, с использованием сети Интернет или даже

интранет, который, при ближайшем рассмотрении, оказывается значительно менее изолированным, особенно при работе физически удаленных подразделений. Следует помнить, что связь может устанавливаться из подразделения, формально не охватываемого СУИБ. Аналогичным образом нужно провести оценку рисков, связанных с физическим доступом сторонних организаций. Также необходимо проанализировать, какие меры предпринимаются для оценки эффективности обеспечения информационной безопасности в сторонней организации, обеспечивают ли средства управления достаточную степень защиты и насколько часто проводится переоценка рисков.

6.2.2.2 Условия безопасности в контрактах, заключенных со сторонними организациями

Соглашения, предусматривающие доступ сторонних организаций к информационным ресурсам организации, должны быть основаны на формальном контракте, в котором должны быть перечислены все необходимые условия безопасности.

Руководство по аудиту:

Аудитору необходимо удостовериться, что все требования по безопасности при ведении дел со сторонними организациями идентифицированы и включены в формальный контракт или соглашение о предоставлении услуг, заключенное между двумя организациями.

6.2.3 Аутсорсинг

Цель: Обеспечить безопасность информации в тех случаях, когда ответственность за обработку информации передается другой организации в соответствии с контрактом на аутсорсинг.

6.2.3.1 Условия безопасности в контрактах на аутсорсинг

В контракте, заключенном между сторонами, должны быть учтены условия безопасности организации, передающей управление и контроль над всеми или некоторыми из своих информационных систем, сетей и/или сред настольных систем.

Руководство по аудиту:

Передача задач по обработке информации в аутсорсинг влечет за собой определенную степень риска в плане безопасности, поскольку организация теряет непосредственный контроль над данными задачами. Одним из способов защиты от рисков, связанных с аутсорсингом, является заключение контракта, в котором четко определены требования по безопасности, средства управления и ответственность обеих сторон. Аудиторам необходимо убедиться в наличии контракта, который покрывает все требования по безопасности в организации. Конкретное содержание контракта определяется на основе оценки рисков.

6.3 Классификация ресурсов и их контроль

6.3.1 Ответственность за ресурсы

Цель: Обеспечить надлежащую защиту ресурсов организации.

6.3.1.1 Инвентаризация ресурсов

Должна быть составлена и должна поддерживаться в актуальном состоянии опись всех важных ресурсов, связанных с каждой информационной системой.

Руководство по аудиту:

Организациям необходимо иметь точную опись ресурсов и поддерживать ее в актуальном состоянии. В опись должны входить все основные информационные и физические ресурсы, программное обеспечение, сервисы и процессы, подлежащие защите. В ходе проверки в первую очередь необходимо убедиться, что ресурсы должным образом идентифицированы и классифицированы. Аудитору следует оценить состояние описи: её полноту и точность, наличие всей необходимой информации, дату и методику обновления, наличие записей о передаче оборудования.

Необходимо удостовериться, что существует лицо, ответственное за инвентаризацию ресурсов. Также нужно проверить, каким образом защищена инвентарная опись: если инвентарная опись ведется в электронном виде, как контролируется доступ и существуют ли резервные копии; если в бумажном – где хранятся документы, как они защищены от потери, что происходит, когда запись необходимо заменить, хранятся ли старые экземпляры, и если да, то в течение какого срока и где они хранятся. Инвентарная опись ресурсов должна четко идентифицировать:

– предмет, с указанием уникального серийного номера, даты и т.п. (там, где это применимо);

– класс безопасности;

– владельца;

– местоположение;

– носитель (для информационных ресурсов);

– дату внесения в опись и/или аудиторской проверки.

6.3.2 Классификация информации

Цель: Обеспечить надлежащий уровень защиты информационных ресурсов.

6.3.2.1 Рекомендации по классификации

Категории информации и связанные с ними защитные средства управления информацией должны учитывать производственную необходимость в коллективном использовании информации или в ограничении доступа к ней, а также воздействие на организацию, связанное с такой необходимостью.

Руководство по аудиту:

Аудиторы должны подтвердить, что организация приложила достаточные усилия для разработки и реализации адекватных принципов классификации. Для нормальной защиты ресурсов необходимо наличие некой формы градации или классификации, в достаточной степени отражающей такие ключевые моменты, как конфиденциальность, целостность и доступность. Схема классификации должна применяться ко всем ресурсам, попадающим в область применения СУИБ. Без четкой системы классификации невозможно обеспечить адекватной защиты ресурсов.

Такая схема не должна быть избыточно сложной и должна подкрепляться соглашениями с другими организациями, которые позволят обеспечить понимание возможных расхождений в классификационных схемах. Предусматривают ли процедуры проверку правильности классификации? Существует ли процедура понижения уровня классификации? Удостоверьтесь, что схема классификации легко доступна, сотрудники осведомлены о ее наличии и понимают принципы классификации, а схема регулярно обновляется. Ответственность за классификацию конкретного ресурса несет его владелец.

6.3.2.2 Маркировка и обработка информации

Должны быть определены процедуры для маркировки и обработки информации в соответствии со схемой классификации, принятой в организации.

Руководство по аудиту:

В организациях должны быть предусмотрены процедуры маркировки и обращения с классифицированной информацией в соответствии с принятой схемой классификации. Аудиторам также следует убедиться, что соответствующей маркировкой выделена наиболее уязвимая информационная единица (например, система обработки информации или база данных).

Маркировка реальных предметов, таких как документация, пленки, аппаратные средства и т.п., является тривиальной задачей, однако как же быть с информацией и корреспонденцией, передаваемой в электронном виде? Необходимо убедиться, что решения, выбранные организацией для маркировки информации в электронном виде, адекватны: есть ли четкие и понятные описания процедур маркировки, правильно ли понимает получатель информации название категории, способствует ли маркировка надлежащей защите информации при ее использовании и хранении? Правильно ли промаркированы физические ресурсы? В ряде случаев инвентарные бирки могут быть неудачно размещены и не сразу заметны; наклейки могут отклеиваться, оставляя предмет без маркировки и стандартной защиты.

6.4 Работа с персоналом по обеспечению информационной безопасности

6.4.1 Безопасность в должностных инструкциях и при выделении ресурсов

Цель: Уменьшить риски ошибки персонала, кражи, мошенничества или неправильного использования оборудования.

6.4.1.1 Безопасность в должностных инструкциях

Обязанности и ответственность за обеспечение безопасности, установленные принятой в организации политикой информационной безопасности, должны быть включены в должностные инструкции.

Руководство по аудиту:

У всех сотрудников, несущих ответственность за конкретные вопросы информационной безопасности, должны иметься должностные инструкции либо эквивалентные им документы, определяющие конкретные обязанности и ответственность за обеспечение безопасности. Аудиторы должны убедиться в том, что такие инструкции существуют, понимание и принятие обязанностей подтверждено подписями самого сотрудника и его руководителя, на документе проставлена дата, а соответствующие вопросы безопасности отражены в нем четко и последовательно. Проверка обязанностей по безопасности, обозначенных в документах политики и описании отдельных процедур, должна показать полное соответствие с должностными инструкциями.

В разных организациях практики хранения должностных инструкций могут отличаться. В одних организациях такие инструкции выдаются непосредственно сотруднику, в других – должностные инструкции хранятся в отделе кадров. В последнем случае следует удостовериться, что сотрудник имеет доступ к данной информации – у сотрудника должен быть собственный экземпляр должностной инструкции, поскольку маловероятно, что человек будет соблюдать предписания документа, который он видел последний раз, возможно, более года назад. Если должность сотрудника подразумевает конкретные обязанности по обеспечению безопасности (например, для системных администраторов), убедитесь, что это надлежащим образом отражено в его должностных обязанностях; стандартные формулировки, относящиеся ко всем сотрудникам, в таких случаях неприемлемы. Также недопустимы устаревшие описания, например, в случае, если сотрудник в настоящий момент выполняет другую работу.

Особенно важно, чтобы новые сотрудники полностью понимали свои обязанности и связанную с ними ответственность; соответствующие документы должны быть оформлены при назначении на должность, а не постфактум. Аудиторам следует обратить особое внимание на временных сотрудников и персонал, работающий по контракту, поскольку у них может не оказаться официально оформленных должностных инструкций. Такая

ситуация недопустима; должностными инструкциями следует обеспечить весь персонал, задействованный в области применения СУИБ.

По крайней мере, следует удостовериться, что все сотрудники подписали договор о соблюдении конфиденциальности (см. 6.4.1.3), а их функции обозначены в контракте. Вопросы безопасности, включенные в должные инструкции, следует тщательно проанализировать, поскольку именно здесь может находиться потенциальное «слабое звено».

6.4.1.2 Проверка принимаемых на работу

При рассмотрении заявлений о приеме на работу должна проверяться достоверность предоставленных сведений для постоянного персонала, сотрудников, работающих по контрактам, и временного персонала.

Руководство по аудиту:

Процедуры набора персонала (включая работающих по контракту и временный персонал) должны включать методику проверки достоверности представленных сведений. В стандарте *СТ РК ИСО/МЭК 17799* приводится список вопросов для рассмотрения; в частности, организации не следует считать представленные сведения достоверными на основе одного лишь резюме, без проведения надлежащих проверок. Любые последующие действия, такие как обсуждения с ответственными за принятие на работу, должны быть зафиксированы документально. Необходимо удостовериться, что руководители осознают свою ответственность в плане оценки и анализа работ, проводимых в организации в сфере их компетенции, в том числе, ответственность за обеспечение безопасности. Также следует убедиться, что вся информация, относящаяся к проверке сведений о сотрудниках, обрабатывается в соответствии с действующим законодательством (защита данных и т.п.).

6.4.1.3 Соглашения о конфиденциальности

В качестве одного из условий приема на работу сотрудники должны подписать соглашение о конфиденциальности.

Руководство по аудиту:

Аудиторам необходимо убедиться, что все сотрудники, относящиеся к области применения СУИБ и имеющие доступ к каким-либо конфиденциальным ресурсам, заключили с организацией соглашение о конфиденциальности. Требуется ли заключать подобное соглашение с посетителями, зависит от того, что именно посетители могут увидеть, и чем они собираются заниматься (см. 6.5.1.2). Аналогичные правила действуют и в отношении временных сотрудников и лиц, работающих по контракту, при предоставлении таковым доступа к конфиденциальной информации.

Как минимум, следует убедиться в наличии обязательств по соблюдению конфиденциальности, зафиксированных в контракте между организацией и поставщиком кадров, и удостовериться, что нанимаемые временно или по контракту сотрудники осведомлены о своих обязательствах.

В целом, контроль за соглашениями о конфиденциальности должен вестись отделом кадров организации, поэтому следует проверить наличие в данном отделе соответствующей формальной процедуры и убедиться в актуальности документов. Особое внимание стоит обратить на наличие подобных соглашений с сотрудниками, недавно уволившимися или собирающимися увольняться.

6.4.1.4 Условия приема на работу

В условиях приема на работу должна быть определена ответственность сотрудника за обеспечение информационной безопасности.

Руководство по аудиту:

Аудиторам необходимо убедиться, что условия приема на работу точно и исчерпывающе описывают ответственность сотрудника за обеспечение безопасности. Соответствующий текст в условиях приема должен охватывать все аспекты безопасности, связанные с конкретной должностью, включая обязанности, связанные с выполнением действующего законодательства, работой вне пределов организации или в нерабочее время, а также обязанности, возможно, выходящие за рамки действия контракта. Условия приема на работу также должны описывать последствия, к которым приведет невыполнение сотрудником собственных обязательств по обеспечению информационной безопасности. В организации должны быть разработаны процедуры по обновлению условий приема на работу при любом изменении обязанностей сотрудника в плане безопасности (например, при расширении круга деятельности или использовании новых информационных систем).

6.4.2 Обучение пользователей

Цель: Обеспечить осведомленность пользователей об угрозах нарушения информационной безопасности и их способность поддерживать принятую в организации политику информационной безопасности в процессе их обычной работы.

6.4.2.1 Обучение правилам информационной безопасности

Все сотрудники организации, а также, при необходимости, пользователи из сторонних организаций должны получить необходимые сведения о принятых в организации политиках и процедурах и об их изменениях.

Руководство по аудиту:

Данное средство управления применимо ко всем сотрудникам, включая пользователей информационных систем, таких как системные администраторы, менеджеры и рядовые пользователи приложений, а также высшее руководство и лица, занимающиеся обработкой любого рода информации (например, бумажной документации, телефонных звонков и т.п.). Первым моментом, на который следует обратить внимание, является адекватность учебных мероприятий имеющимся задачам; учебные мероприятия должны соответствовать требованиям конкретной должности и связанным с ней обязанностям по обеспечению безопасности. Как

проводится обучение, с использованием внутренних или внешних ресурсов организации? Если обучение проводится собственными силами организации, что оно собой представляет: формальный учебный курс или стандартное обучение «в процессе работы»? Кто проводит обучение, и имеют ли эти лица необходимую квалификацию? Если обучение проводится неформально, определен ли круг рассматриваемых тем? Если обучение проводится вне организации, кем утверждены проводящие обучение лица/учреждения? В каких документах зафиксированы учебные мероприятия, и отражают ли эти документы тематику и уровень обучения?

В минимальном варианте, для всех сотрудников организации в той или иной форме должен проводиться вводный тренинг. Он должен охватывать общие принципы и политику безопасности, сферы применения и т.п. Такой тренинг должен быть формально зафиксирован в учетных карточках сотрудников. Кроме того, необходимо в достаточном объеме обеспечить проведение учебных мероприятий для сотрудников, ответственных за серьезные вопросы безопасности, и проследить, чтобы использовались актуальные учебные материалы, а график обучения был составлен с учетом предстоящих работ.

Возможны ситуации (в особенности, в связи с техническими аспектами), когда сотрудники ссылаются на предыдущий опыт или ранее полученную аттестацию в качестве замены формальному обучению. Аудиторам следует подходить к этому прагматически и при оценке навыков сотрудников и их соответствия выполняемым функциям принимать во внимание сумму знаний, полученных в результате формального обучения, квалификационных испытаний и на основе опыта. Если сотрудник ссылается на имеющийся опыт работы, следует удостовериться, что полученные знания не устарели и релевантны. Необходимо выяснить, в какой среде был получен этот опыт и проводилась ли какая-либо проверка знаний сотрудника. Многие организации слишком сильно рассчитывают на правдивость сведений, сообщенных о себе сотрудником в резюме. Однако не имеющий достаточной квалификации или опыта человек, принятый на ключевую должность, может нанести серьезный урон жизненно важным ресурсам организации, поэтому постарайтесь, чтобы к этому вопросу подошли серьезно. Данная проблема имеет отношение к проверке принимаемых на работу (см. 2.4.1.2).

6.4.3 Реагирование на сбои и инциденты в системе безопасности

Цель: Минимизировать ущерб от инцидентов в системе безопасности и ее сбоев, а также отслеживать такие события и извлекать из них соответствующие уроки.

6.4.3.1 Уведомление об инцидентах в системе безопасности

Об инцидентах в системе безопасности следует незамедлительно сообщать по административным каналам.

Руководство по аудиту:

Во всех организациях должны быть предусмотрены соответствующие процедуры и административные каналы для оповещения об инцидентах безопасности. Аудиторам следует убедиться, что такие процедуры охватывают все возможные виды инцидентов и предусматривают адекватные ответные меры. Если в организации утверждают, что инцидентов, требующих оповещения, не происходит и, соответственно, они не могут продемонстрировать процесс оповещения, скорее всего, инциденты все же происходили – просто они остались незамеченными. Таким образом, процедуры оповещения об инцидентах должны иметься в наличии вне зависимости от наличия инцидентов безопасности в прошлом.

Удостоверьтесь, что в соответствующей документации четко описано, что является инцидентом, а что нет, и ответственные сотрудники хорошо понимают принятое в организации определение инцидента. Может оказаться полезным рассмотреть несколько примеров: «Считаете ли вы, что произошел инцидент безопасности, если в помещении организации обнаружен неохраняемый открытый сейф?»; «Если сотрудник сообщил, что по ошибке получил чужую зарплатную ведомость, можно ли считать это инцидентом безопасности?» и т.п. Очевидно, что такие примеры должны быть применимы к конкретной ситуации, однако ответы сотрудников могут быть достаточно показательными и отражать общий подход к таким вопросам. В случае, если организация предоставила отчеты об инцидентах, проанализируйте, какая реакция последовала на произошедший инцидент: был ли он урегулирован, производилось ли расследование причин и извещен ли о результатах расследования сотрудник, сообщивший об инциденте (конечно, если эта информация не является конфиденциальной).

6.4.3.2 Уведомление о слабых местах в системе безопасности

Пользователи информационных сервисов обязаны регистрировать любые наблюдаемые или предполагаемые слабые места в защите систем или сервисов либо угрозы системам и сервисам и сообщать о них.

Руководство по аудиту:

Для оповещения о предполагаемых или реальных слабых местах в защите должны быть предусмотрены процедуры уведомления, аналогичные тем, что используются для инцидентов безопасности. Все сотрудники должны осознавать необходимость оповещения о слабых местах в защите безопасности. Это относится не только к области систем обработки информации – открытое окно в помещении также может представлять собой слабое место в защите. Процедуры уведомления должны включать в себя инструкции для сотрудников, запрещающие им использовать обнаруженные слабости, например, для получения несанкционированного доступа. Даже если их целью является всего лишь подтвердить наличие слабого места в защите, такие действия могут нанести серьезный ущерб.

6.4.3.3 Уведомление об отказах программного обеспечения

Должны быть разработаны процедуры уведомления об отказах программного обеспечения.

Руководство по аудиту:

Данные проблемы могут подпадать под описанные выше процедуры по работе с инцидентами безопасности и потенциальными слабостями в защите, однако следует убедиться, что форма уведомления требует от пользователя явного указания признаков сбоя и любых сообщений, выданных компьютером, – эти данные помогут в расследовании причин отказа ПО. Процедуры уведомления (так же, как и в случае с инцидентами безопасности и слабыми местами в защите) должны обеспечить оповещение ответственных лиц о любых сбоях, так как то, что одни пользователи воспринимают как мелкие неприятности, может оказаться серьезной проблемой безопасности при анализе компетентными специалистами.

Своевременность уведомления крайне важна; например, раннее оповещение о возможном заражении вирусом может позволить избежать огромного ущерба. Аудиторам необходимо тщательно проанализировать коррекционные мероприятия (возможно, соответствующее ПО можно исправить, в других случаях необходимо ожидать выхода новой версии, и следует искать обходные пути решения проблемы): насколько эффективны принятые меры, требуется ли изменение каких-либо других процедур, как информация о данной ситуации распространяется среди заинтересованных лиц. Утверждены ли временные изменения, которые могут потребоваться? Если ситуация требует вовлечения сторонних лиц/учреждений (например, поставщика программного обеспечения), каким образом им предоставляется информация, и не появляется ли в процессе передачи информации отдельная проблема для безопасности организации?

Уведомления и отчеты об инцидентах безопасности, слабых местах в защите и сбоях программного обеспечения направляются соответствующему контактному лицу или лицам. Необходимо проверить, что выбранные контакты являются наиболее подходящими, доступны в нужный момент и обладают соответствующими знаниями. Рассматриваются ли уведомления достаточно внимательно, как определяется приоритет проблемы, имеются ли явные процедуры назначения высокого приоритета, присутствует ли обратная связь с лицами, сообщившими о проблеме?

6.4.3.4 Извлечение уроков из инцидентов

Должны быть реализованы механизмы для количественной оценки и мониторинга типов, масштабов и стоимости инцидентов и сбоев.

Руководство по аудиту:

Аудиторам следует проанализировать все примеры реагирования на инциденты безопасности и сбои программного обеспечения и систем, имевшие место в организации в прошлом. Необходимо выяснить, как

проводится количественная оценка и определение масштаба инцидентов, а также насколько процедуры работы с инцидентами соответствуют инцидентам, происходившим ранее, и предполагаемым типам инцидентов в будущем.

Если организация утверждает, что для извлечения уроков произошло недостаточное количество инцидентов или отсутствует релевантная информация, к таким заявлениям следует подходить с осторожностью, поскольку они могут сигнализировать об отсутствии или неиспользовании процедур уведомления об инцидентах. В таком случае аудитору необходимо произвести дополнительный анализ ситуации и обсудить ее с надлежащими лицами в организации.

В организации должны быть предусмотрены планы и процедуры реагирования на инциденты безопасности и сбои программного обеспечения и систем. В них должна входить реализация дополнительных средств управления и процедур, позволяющих предотвратить повторное появление проблем, ограничить ущерб, обеспечить сбор необходимых свидетельств и добиться более оперативного и эффективного реагирования в будущем. Извлечение уроков из инцидентов также предполагает их использование в рамках тренингов и ознакомительных программ по безопасности в качестве реальных примеров.

6.4.3.5 Дисциплинарная процедура

Нарушение сотрудниками принятых в организации политик и процедур безопасности должно рассматриваться в рамках формальной дисциплинарной процедуры.

Руководство по аудиту:

Для организации данный вопрос может быть достаточно щекотливым, однако для адекватного реагирования на нарушения безопасности крайне важно, чтобы соответствующая процедура была предусмотрена. Детали дисциплинарной процедуры, а также гарантии справедливого рассмотрения для всех задействованных лиц должны быть доведены до сведения сотрудников. Если дисциплинарная процедура реализована некорректно, существует вероятность предъявления претензий в связи с несправедливым увольнением или другими нарушениями прав сотрудников. В любом случае, четко определенная дисциплинарная процедура является сдерживающим фактором, без которого эффективность управления может существенно снизиться. Аудиторам следует проанализировать зарегистрированные инциденты безопасности, рассмотреть критерии применения дисциплинарных взысканий и удостовериться, что данные процедуры применяются эффективно.

6.5 Физическая безопасность и безопасность среды функционирования

6.5.1 Защищенные области

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

6.5.1.1 Физический периметр безопасности

Организации должны использовать периметры безопасности для защиты областей, в которых размещаются средства обработки информации.

Руководство по аудиту:

Все организации должны продемонстрировать способы и средства физической защиты своих ресурсов. Если речь идет о крупных объектах, процедуры безопасности должны описывать, какие принимаются меры защиты, как они контролируются и у кого имеется доступ к объекту. Для оценки реализованной в организации физической защиты аудиторам следует проанализировать возможные бреши: открытые пожарные выходы/лестницы, неконтролируемые помещения для приема посетителей, использование чужих пропусков и незапертые шкафчики – все это представляет потенциальную угрозу безопасности и должно быть соответствующим образом зафиксировано.

Частью реализации физической защиты является использование физических периметров, поэтому организация должна предоставить сведения об имеющихся физических периметрах и защите, которую они предоставляют (эта информация должна подкрепляться данными по оценке рисков). Аудиторам также следует выяснить, как предоставляется и контролируется доступ в здание, где размещается организация и насколько используемые средства управления достаточны для ее нужд, а также поинтересоваться наличием возможности обойти средства защиты.

6.5.1.2 Контроль доступа в помещения

Защищенные области должны быть защищены необходимыми средствами контроля доступа в помещения, чтобы к ним имел доступ только персонал, получивший соответствующие полномочия.

Руководство по аудиту:

Аудиторам необходимо проверить реализацию контроля доступа в помещение и убедиться, что этого достаточно для ограничения физического доступа для всех лиц, не имеющих соответствующего разрешения. Носят ли сотрудники идентификационные карточки (бэджи), и является ли их ношение обязательным? Выдаются ли аналогичные бэджи посетителям, регистрируется ли их приход/уход, какие ограничения накладываются на их перемещения в пределах организации? Останавливаются ли лица без бэджей

для проверки? Последнее аудиторы, сами являющиеся посетителями, могут проверить на собственном опыте.

Аудиторам также следует проверить старые регистрационные записи по доступу и убедиться, что в организации предусмотрены процедуры проверки и обновления прав физического доступа в помещения. Разрешение или запрет на физический доступ могут быть выражены в разной форме: они могут включаться в должностные инструкции, присутствовать в описании процедур или обозначаться непосредственно там, где ограничения вступают в силу (например, табличка на двери в помещение, куда ограничен доступ). Аудиторам следует оценить приемлемость каждого из таких подходов.

6.5.1.3 Защита офисов, комнат и оборудования

Для защиты офисов, комнат и оборудования, к безопасности которых предъявляются особые требования, должны быть созданы защищенные области.

Руководство по аудиту:

Уровень защиты, обеспечиваемый для защищенной области, должен соответствовать максимальной степени конфиденциальности информации, которая будет там храниться, согласно процедурам работы с конфиденциальной информацией. Этот момент напрямую связан с оценкой рисков, и аудиторам следует удостовериться, что требования по обеспечению информационной безопасности идентифицированы, а реализованные средства защиты соответствуют им.

Кроме контроля доступа, аудиторам необходимо исследовать прочие аспекты безопасности и доступности, такие, как подача электроэнергии, защита в чрезвычайных ситуациях, защита от природных явлений (есть ли угроза пожара, может ли помещение подвергнуться затоплению), и выяснить, как предполагается предотвратить эти опасности или минимизировать их последствия. См. также разделы «Размещение и защита оборудования» и «Источники электропитания» (п. 6.5.2).

6.5.1.4 Работа в защищенных областях

В целях повышения безопасности защищенных областей должны использоваться дополнительные средства контроля и правила работы в защищенных областях.

Руководство по аудиту:

Для сотрудников, работающих в защищенных областях, должны применяться особые средства управления, обеспечивающие реализацию уровня безопасности, достаточного для защиты конфиденциальной и критичной для организации информации, с которой там ведется работа. Аудиторам необходимо проверить:

– наличие средств контроля физического доступа, позволяющих обеспечить доступ в защищенные области только лиц, имеющих специальное разрешение;

– насколько подробно известно сотрудникам компании о работах, ведущихся в защищенных областях, и не выходит ли эта информация за рамки необходимого минимума сведений;

– насколько легко пронести информацию в защищенную зону или вынести данные из нее (информация может содержаться в бумажной документации или быть записанной на диске);

– возможно ли пронести в защищенную зону фотографическое, видео-, аудио- или любое другое записывающее оборудование, а также использовать его для записи в ручном или автоматическом режиме;

– осуществляется ли контроль за работами в таких зонах в достаточном объеме, и предусмотрены ли механизмы двойного контроля в случаях, когда таковой требуется.

6.5.1.5 Изолированные места разгрузки и погрузки

Места разгрузки и погрузки должны контролироваться и по возможности изолироваться от средств обработки информации в целях предотвращения несанкционированного доступа.

Руководство по аудиту:

Данное средство управления призвано предотвратить инциденты безопасности при операциях разгрузки и погрузки. Доставка грузов может производиться сторонним персоналом, чьи перемещения по территории организации необходимо ограничить. Доставленные грузы могут представлять опасность, если при их получении не был проведен первоначальный осмотр и тестирование или при несоблюдении условий хранения. В грузы, вывозимые с территории организации, может непреднамеренно попасть конфиденциальная информация. Все области риска, применимые к конкретной ситуации, должны быть выявлены на основе оценки рисков, а организация должна принять адекватные меры для предотвращения потенциальных нарушений безопасности и минимизации их последствий. Например, кем осуществляется приемка доставленных грузов: сотрудником, для которого они предназначаются, складским работником или секретарем в приемном помещении? Что происходит с доставленными грузами: они сразу транспортируются в защищенную зону, отправляются на склад или доставляются адресату напрямую?

6.5.2 Защита оборудования

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

6.5.2.1 Размещение и защита оборудования

Оборудование должно быть размещено или защищено так, чтобы уменьшить риск, связанный с воздействием внешней среды и возможностью несанкционированного доступа.

Руководство по аудиту:

Организации должны продемонстрировать, как защищено используемое ими оборудование. Оборудование должно размещаться вдали от потенциальных зон риска, таких, например, как окна, через которые легко проникнуть внутрь помещения, не вызвав срабатывания сигнализации. Также следует учесть, что экраны компьютерных терминалов могут просматриваться из-за пределов защищенной области.

В ряде ситуаций может потребоваться зафиксировать компьютерное оборудование на рабочих столах сотрудников. Помимо защиты от злонамеренной порчи, оборудование требуется оградить от случайного ущерба, вызванного беспорядком в помещении, неконтролируемого доступа, неустойчивой мебели, пролитой жидкости и т.п., а также от неблагоприятного воздействия окружающей среды: воды, химикатов, огня. Проверьте, что в организации разработаны и реализованы соответствующие защитные меры.

Проверка не должна ограничиваться одними местами, в которых расположена компьютерная техника. Выясните, существует ли угроза пожара или затопления в соседних помещениях. В крупных организациях обычно имеется план здания (помещения). Ознакомьтесь с ним и оцените адекватность размещения оборудования с точки зрения безопасности.

6.5.2.2 Источники электропитания

Оборудование должно быть защищено от сбоев в системе электропитания и других неполадок в электрической сети.

Руководство по аудиту:

Необходимый уровень защиты от перебоев в подаче электроэнергии зависит от требований безопасности и критичности хранимой информации, а также оборудования в составе системы (например, при высоких требованиях по доступности системы необходимо использование более серьезных средств управления для обеспечения электропитания). В любом случае аудиторам необходимо удостовериться, что реализована хотя бы минимальная степень защиты – выравнивание скачков напряжения.

При наличии более серьезных требований, проверьте наличие достаточных резервных источников питания и систем резервного копирования: дополнительных генераторов, ИБП, дисковых RAID-массивов и т.п. Если таковые наличествуют, обратите внимание на следующие моменты: достаточно ли вырабатывается электроэнергии по резервной схеме; в течение какого времени резервные источники обеспечивают работоспособность оборудования; соответствует ли этот период контрактным обязательствам организации; соблюдаются ли рекомендации производителя при обслуживании и тестировании систем резервного питания. Аудитор также должен проверить, обеспечиваются ли помещения организации аварийным освещением на случай отключения электроэнергии.

6.5.2.3 Защита кабельной сети

Кабели электропитания и сетевые кабели, используемые для передачи данных или поддержки информационных сервисов, должны быть защищены от возможности перехвата информации или повреждения.

Руководство по аудиту:

Необходимо оценить общее состояние кабельных соединений и разъемов: правильно ли они скоммутированы и проложены, нет ли опасности повреждения из-за неправильного размещения кабеля, и т.п.

Разводка коммуникационных соединений может быть критическим моментом для части пользователей. Аудиторам следует выяснить, какие риски связаны с вопросами коммуникации, и идентифицировать потенциальные слабости защиты: сетевые кабели, проложенные между отделами или зданиями, телефонные линии, незащищенные от возможных повреждений или прослушивания.

6.5.2.4 Техническое обслуживание оборудования

Должно осуществляться надлежащее техническое обслуживание оборудования в целях обеспечения его постоянной доступности и целостности.

Руководство по аудиту:

Аудиторам следует убедиться, что в организации реализованы средства управления, позволяющие обеспечить обслуживание оборудования с периодичностью, рекомендованной поставщиком, и в соответствии с представленными спецификациями. Кроме того, регулярное проведение таких простых мероприятий, как чистка воздушных фильтров, механических деталей накопителей на магнитной ленте и принтеров, может помочь предотвратить серьезные поломки. Даже такие рядовые операции, как регулярная дефрагментация жестких дисков компьютеров, могут оказать существенное влияние на эффективность работы.

Выясните, какие мероприятия по обслуживанию предусмотрены принятыми в организации процедурами, определите, достаточны ли они, и проверьте имеющиеся записи по обслуживанию, чтобы убедиться в их соответствии обозначенным процедурам. В организации должен быть предусмотрен формальный механизм уведомления о сбоях. Убедитесь в его наличии, а также проверьте записи об обнаруженных дефектах и их устранении. Необходимо удостовериться, что мероприятия по сервисному обслуживанию оборудования могут производиться исключительно персоналом, имеющим соответствующее разрешение, а любых сторонних лиц, участвующих в процедурах по обслуживанию, сопровождают ответственные сотрудники.

6.5.2.5 Защита оборудования, используемого за пределами организации

Любое использование оборудования для обработки информации вне помещений организации должно быть санкционировано руководством.

Руководство по аудиту:

Данное средство управления обеспечивает безопасность любого оборудования, которое используется за пределами территории организации. Для части организаций, в зависимости от рода их основной деятельности, эта проблема не является актуальной, однако для большинства учреждений данный вопрос достаточно существенен.

Использование оборудования за пределами защищенной среды в организации связано с множеством проблем в области безопасности и дополнительными угрозами. Поэтому аудиторам необходимо удостовериться, что средства управления, ориентированные на обеспечение физической безопасности за пределами основной территории, обеспечивают достаточный уровень защиты, сопоставимый со стандартным уровнем безопасности в организации. Должны быть предусмотрены процедуры и рекомендации, гарантирующие, что оборудование за пределами основной территории не будет оставлено без контроля, а при необходимости будет обеспечена адекватная страховка.

6.5.2.6 Надежная утилизация или повторное использование оборудования

Перед утилизацией или повторным использованием оборудования с него следует удалить информацию.

Руководство по аудиту:

В организации должен быть предусмотрен эффективный процесс удаления данных с оборудования, предназначенного для утилизации, и прочего оборудования, тем или иным образом выходящего из-под контроля. Аудиторам следует удостовериться, что пользователи понимают возможные опасности в подобной ситуации, а у организации имеются эффективные средства, позволяющие гарантировать, что предназначенные для утилизации устройства не содержат конфиденциальной информации. Удаление файлов с магнитных носителей не является безопасной практикой: в ряде случаев данные все равно доступны после стирания. Прежде, чем данные полностью исчезнут, может потребоваться неоднократное форматирование или перезапись информации. Для систем, требующих максимальной защиты, может потребоваться специальное оборудование по уничтожению данных на дисках и магнитных лентах. Соответствующая политика может распространяться на все виды носителей – например, с носителей, содержащих конфиденциальную информацию, может потребоваться удаление всех надписей/наклеек, чтобы максимально затруднить их идентификацию.

В зависимости от имеющихся рисков самым надежным способом может оказаться физическое уничтожение дискет и магнитных лент; это также может распространяться на жесткие диски, установленные в компьютерах. Некоторые организации могут счесть такой подход чересчур радикальным, однако магнитные носители информации относительно недороги, и в любом

случае их уничтожение явно принесет меньший финансовый ущерб, чем потеря компрометирующих или конфиденциальных данных. Также следует обратить внимание на оборудование, отдаваемое для починки в сервис: проводятся ли проверки на возможность доступа или модификации важной информации?

6.5.3 Общие средства управления

Цель: Предотвратить компрометацию или кражу информации и оборудования информационных систем.

6.5.3.1 Политика использования рабочего стола и компьютерных терминалов

Организации должны установить правила использования рабочего стола и компьютерных терминалов, направленные на уменьшение риска несанкционированного доступа к информации, ее потери и повреждения.

Руководство по аудиту:

Целью данного средства управления является гарантировать, что конфиденциальная информация любого рода (в электронной, бумажной форме, записанная на носитель и т.п.) не будет оставляться без надлежащего контроля, а также обеспечить защиту информации от потери (а значит, от компрометации, модификации, и недоступности). Предусмотренные меры должны применяться как в рабочее, так и в нерабочее время. Также необходимо надлежащим образом классифицировать информацию, в соответствии с принципами, описанными в разделе «Классификация информации».

Необходимо принять меры защиты, учитывающие опасность доступа к конфиденциальной информации со стороны внешнего персонала (например, уборщиков). Также необходимо проверить, что происходит в то время, когда столы, шкафы для бумаг, сейфы и т.п. оставляются без присмотра в течение рабочего дня: представляет ли такая ситуация проблему, не приводит ли она к нарушениям безопасности? Кроме того, следует подумать о доступе к компьютерам в отсутствие сотрудников вне зависимости от продолжительности их отсутствия. В такой ситуации необходимо использовать защищенные паролем хранители экрана, выключать компьютер или применять любые другие средства управления, предусмотренные политикой использования компьютерных терминалов.

В ряде случаев необходимо применение дополнительных средств управления логическим доступом, описанных в разделе «Средства управления». Если для всей зоны обеспечивается соответствующий уровень безопасности, а находящиеся в ее пределах сотрудники прошли проверку на входе, введение дополнительных мер может не потребоваться. Проверьте, что в целом политика сформулирована четко, а сотрудники осведомлены о соответствующих процедурах и следуют им.

6.5.3.2 Вынос имущества за пределы организации

Вынос оборудования, информации или программного обеспечения, принадлежащих организации, за пределы организации должен быть санкционирован руководством.

Руководство по аудиту:

Специфика деятельности многих организаций может требовать от сотрудников выноса оборудования, данных и документации за пределы территории на регулярной основе.

Это может требоваться при надомной работе, проведении встреч и совещаний и т.п. Для ряда организаций контроль таких перемещений может представлять проблему. Аудитору прежде всего следует убедиться, что в организации идентифицировали как саму проблему, так и эффективные средства управления для ее решения. Существует несколько возможных вариантов:

– Вынос любой конфиденциальной информации запрещен. На первый взгляд, это самый простой подход, однако для большинства организаций его крайне трудно реализовать. Такое решение может потребоваться организациям с самыми строгими требованиями по безопасности.

– Вынос конфиденциальной информации допускается в соответствии с избранными средствами управления. Здесь от организации требуется предельно четкое определение допустимой к выносу информации и строгий перечень необходимых средств управления.

– Вынос конфиденциальной информации никак не контролируется. Этот вариант может представлять большую опасность, и его реализация не рекомендуется при отсутствии дополнительных средств управления, регулирующих работу с конфиденциальной информацией за пределами организации.

Аудитору следует определить, какой подход выбран в политике организации, а затем ознакомиться с соответствующими документированными процедурами. Используется ли система регистрации при проносе/выносе имущества, какие требуются разрешения и где они фиксируются, применяются ли эти правила для всех предметов, или только для ограниченного подмножества? Как отслеживается соблюдение норм со стороны руководства? Чрезмерно строгий режим может привести к желанию обходить принятые процедуры, а слишком мягкий режим вызовет очевидные нарушения безопасности. Предусматривает ли соглашение о конфиденциальности ответственность за информацию во владении сотрудника вне территории организации? Многие сотрудники пользуются портативными компьютерами: какие средства управления реализованы в организации для работы с ними и содержащимися в них конфиденциальными данными? Информация, записанная в память компьютера или на электронном носителе, может быть замаскирована (например, изменением

имен файлов); требуются ли для борьбы с этим поисковые средства, и если да, когда необходимо их применять?

Доступность средств коммуникации в современном мире означает, что для выноса информации за пределы организации не обязательно использование физических носителей; аудиторам следует выяснить, какие механизмы контроля передачи данных используются, например, при доступе к сети Интернет.

6.6 Администрирование компьютерных систем и вычислительных сетей

6.6.1 Операционные процедуры и обязанности

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

6.6.1.1 Документированные операционные процедуры

Операционные процедуры, идентифицированные в политике безопасности, должны быть задокументированы и утверждены.

Руководство по аудиту:

Аудиторам необходимо изучить и проанализировать операционные процедуры организации на предмет адекватного отражения в документации и последовательного применения во всех частях организации, где это необходимо. Для того чтобы проверить полноту данных процедур, аудиторам потребуется иметь общее представление о различных операционных процессах и работе организации.

Дополнительно необходимо проверить использование, поддержку и выполнение этих процедур. Следует также провести проверку, гарантирующую невозможность внесения изменений в процедуры без соответствующих санкций, а также невозможность обойти их и любые связанные с ними средства управления.

Ответственность за эксплуатацию и администрирование сетевых сервисов обычно лежит на отдельном подразделении или даже отдельной организации. Соответственно, аудитору необходимо понимать, каким образом этот вопрос решен в организации, и убедиться, что сервисные мероприятия и процедуры адекватно документированы на соответствующем уровне. В некоторых областях потребуются подробные инструкции по проведению работ. Также весьма вероятно, что в процессе эксплуатации и администрирования будет активно использоваться документация поставщиков оборудования, поэтому следует проверить ее наличие и актуальность.

6.6.1.2 Контроль изменений

Все изменения в средствах и системах обработки информации должны контролироваться.

Руководство по аудиту:

Аудитору необходимо убедиться в наличии ответственных лиц и формальных процедур по контролю изменений в функционирующих средствах обработки информации. Все такие изменения должны отслеживаться, а подробности о конкретных изменениях регистрироваться в соответствующем протоколе. Необходимо гарантировать, что ни одно изменение не может быть произведено без оценки возможного ущерба от его введения, а каждое предложенное изменение будет соответствующим образом утверждено.

В организации должны быть предусмотрены процедуры, описывающие порядок реагирования в проблемной ситуации; также следует гарантировать, что работы по внесению изменений начнутся только при наличии соответствующих процедур отката, которые при необходимости позволят вернуться к первоначальному состоянию. Аудиторам следует убедиться, что процедуры предусматривают информирование всех заинтересованных сотрудников о внесенных изменениях. Если операционные изменения также приводят к изменениям в приложениях, такие изменения необходимо интегрировать.

6.6.1.3 Процедуры реагирования на события

Для обеспечения своевременного, эффективного и организованного реагирования на инциденты в системе безопасности и для сбора данных, связанных с инцидентами (таких, как контрольные журналы), должны быть определены соответствующие процедуры и административные обязанности.

Руководство по аудиту:

Аудитору следует проверить наличие процедур реагирования на события (процедур по работе с инцидентами), а также их соответствие схеме оповещения, описанной в разделе «Уведомление об инцидентах в системе безопасности».

Проверьте, что все мероприятия хорошо документированы в описании процедур, присутствует соответствующий контроль со стороны руководства, а данные по инцидентам и ответным мероприятиям надлежащим образом регистрируются.

6.6.1.4 Разделение обязанностей

Для уменьшения вероятности несанкционированной модификации или ненадлежащего использования информации или сервисов должно быть реализовано разделение обязанностей и зон ответственности.

Руководство по аудиту:

Для небольших организаций в данном вопросе могут возникнуть сложности; кроме того, в данном разделе выделяются типичные обязанности, для которых рекомендуется применять принцип разделения. Для более крупных учреждений принцип разделения должен являться установленным фактом, соответствующим образом отраженным в процедурах. Из всех областей, перечисленных в стандарте независимых операций, обеспечение и

аудит безопасности, пожалуй, являются наиболее важными и должны рассматриваться в первую очередь.

Аудитору следует выяснить, какие независимые проверки данных и результатов проводятся между стадиями обработки или перед выпуском. В рамках подробного анализа рисков организация должна была рассмотреть критичные процессы и проверить, нет ли сотрудников, единолично ответственных за слишком большое число проверок и корректировок. Рассмотрите рабочие процедуры для критичных задач: как решается ситуация с отсутствием по болезни или праздниками, не ставят ли такие ситуации под угрозу независимость операций? Для эффективной реализации принципа разделения обязанностей в организации может потребоваться введение обязательных праздничных периодов.

6.6.1.5 Разделение средств разработки и рабочих средств

Средства разработки и тестирования должны использоваться отдельно от рабочих средств. Должны быть определены и задокументированы правила по переводу программного обеспечения из статуса программы для разработки в статус рабочей программы.

Руководство по аудиту:

Для небольших организаций выполнение данных требований может оказаться непростым, однако, чтобы не допустить перерывов в рабочем процессе, обеспечение такого разделения крайне важно. Соответственно, аудитору необходимо выяснить, как реализовано разделение и какие процедуры утверждения гарантируют, что находящееся в процессе разработки или непротестированное программное обеспечение не используется на рабочих системах.

Если рабочие приложения и информация хранятся на той же компьютерной системе, что и разрабатываемое и тестируемое ПО, аудитор должен удостовериться, что используются мощные средства управления, не допускающие смешивания новых разработок и рабочих средств.

Для рабочих тестировочных систем и систем разработки могут потребоваться разные учетные записи и пароли; инструменты разработчика, такие как компиляторы, системные утилиты, средства редактирования программ и т.п., не должны быть доступны из рабочих систем. Проверьте, как вводится в эксплуатацию новое программное обеспечение, и убедитесь, что новое ПО не находится на стадии разработки или тестирования.

6.6.1.6 Администрирование сторонними организациями

Перед использованием услуг сторонних организаций по администрированию риски должны быть идентифицированы, а соответствующие средства управления согласованы с подрядчиком; эта информация должна быть внесена в контракт.

Руководство по аудиту:

Организации, пользующиеся сторонними услугами администрирования систем (АС), должны в полном объеме выполнить указанные выше требования. Для идентификации требований по безопасности и необходимых средств управления нужно провести анализ рисков, затем переговоры по заключению контракта или подписанию сервисного соглашения и, наконец, произвести мониторинг производительности.

Аудитору необходимо убедиться, что при использовании организацией услуг по АС, перечисленные выше вопросы решены. Также следует проанализировать результаты мониторинга: каким образом организация контролирует адекватность работы с важной и конфиденциальной информацией? Есть ли у них информация о процедурах, которые используются в организации АС, как в плане безопасности, так и общих принципов работы? Что они знают о персонале, который имеет доступ к их системам?

6.6.2 Планирование систем и их приемка

Цель: Минимизировать риск отказов систем.

6.6.2.1 Планирование нагрузки

Для обеспечения надлежащей производительности систем и емкости запоминающих устройств должен осуществляться мониторинг нагрузки и должны разрабатываться прогнозы относительно будущих требований к нагрузке.

Руководство по аудиту:

Организации зачастую пренебрегают заблаговременным планированием основных операционных потребностей, поэтому аудиторам необходимо оценить возможности организации по устранению данной проблемы. Первым следует задать вопрос: «Какие параметры отслеживаются?» Обычно это бывает емкость дисковых накопителей или других устройств хранения данных, пропускная способность при передаче информации, использование принтеров и другие возможные «узкие места».

Затем необходимо проанализировать, как информация, полученная с помощью мониторинга, используется для оценки будущих требований по производительности. Отслеживание тенденций и экстраполяция текущих требований позволит произвести плановое обновление аппаратных средств с минимальными перерывами в работе. Сюда входит получение данных по требуемой производительности на основе анализа тенденций, а также проверка и идентификация потребностей и планов по обновлению оборудования. Также следует проверить планирование потребностей в рабочей силе. Недостаточные кадровые ресурсы могут привести к нарушениям безопасности в критической ситуации.

6.6.2.2 Приемка систем

Критерии приемки новых информационных систем, модернизаций и новых версий должны быть разработаны и надлежащим образом проверены до момента приемки.

Руководство по аудиту:

Внедрение новых систем или обновление уже существующих требует тщательного планирования. Необходимо осуществлять строгий контроль ввода новых систем, обновления оборудования и установку новых версий программного обеспечения, чтобы не допустить остановки сервисов или компрометации данных в уже работающих системах.

Аудиторам нужно выявить четкие критерии приемки, которые необходимо удовлетворить перед внедрением новых систем или обновлением старых. Перед вводом в эксплуатацию новые системы или процессы должны пройти тщательную проверку: какие тестовые планы предусмотрены, проверена ли их адекватность, каким образом зафиксированы полученные результаты?

Достаточный объем тестирования подразумевает нечто большее, чем простая проверка новой функциональности; выясните, достаточное ли внимание было уделено регрессионным тестам, проводилось ли тестирование реакции системы на некорректные данные или ошибки пользователей при вводе, полностью ли обеспечена безопасность в плане контроля доступа, проверялись ли другие средства управления безопасностью?

Вместе с приемкой системы могут проводиться тренинги; предусмотрена ли такая возможность, кто определял объемы обучающих мероприятий, все ли заинтересованные сотрудники охвачены при подготовке и проведении тренинга? Кто санкционирует окончательную приемку перед вводом в эксплуатацию? Проверьте, что данные моменты четко определены и документально зафиксированы.

6.6.3 Защита от вредоносного программного обеспечения

Цель: Обеспечить целостность информации и программного обеспечения.

6.6.3.1 Средства защиты от вредоносного программного обеспечения

Должны быть реализованы средства обнаружения и предупреждения, обеспечивающие защиту от вредоносного программного обеспечения, а также должны быть разработаны соответствующие процедуры по информированию пользователей.

Руководство по аудиту:

Вредоносное программное обеспечение представляет собой проблему почти для всех операционных систем; соответственно, аудитору необходимо убедиться в полной адекватности всех необходимых средств управления. Существует несколько вариантов установки программных средств защиты от вредоносного ПО: иногда защитные программы устанавливаются на сервере

и работают для всех подключенных в данный момент клиентских систем, другие программы требуют локальной установки на каждой отдельной рабочей станции. При установке обновлений часть ПО заменяется полностью, в то время как в других продуктах обновления затрагивают лишь определенные библиотеки и базы; соответственно, аудиторы должны понимать, как правильно определить текущую версию программного обеспечения в каждом конкретном случае.

Еще одним важным моментом, требующим проверки, является регулярность установки необходимых обновлений: используется ли система автоматического обновления или какой-либо другой метод оповещения о необходимости обновить защитное ПО. Работа с портативными вычислительными устройствами может представлять дополнительную проблему: каким образом для них гарантируется регулярная установка обновлений? Если поиск обновлений не работает постоянно в фоновом режиме (один из предпочтительных вариантов, который, к сожалению, не всегда имеется возможность реализовать), в процедуры должна быть в явной форме включена регулярная проверка наличия обновлений. Кроме того, в организации должна быть предусмотрена четкая политика относительно загружаемого программного обеспечения.

Принятые в организации процедуры должны описывать необходимые действия в случае заражения компьютерным вирусом. Все факты появления вредоносных программ должны надлежащим образом регистрироваться. Проверьте, какое защитное программное обеспечение используется: обеспечивает ли оно требуемый уровень защиты, и осуществляется ли для такого ПО необходимая техническая поддержка?

Бесплатные программные пакеты (например, доступные для загрузки через Интернет) не всегда обеспечивают необходимую защиту безопасности, а в редких случаях могут привести к дополнительному ущербу. Убедитесь, что операторы рабочих станций осведомлены о правильных методах работы с защитным ПО, приложениями, операционными системами и т.п. и применяют эти методы на практике – например, запрос пароля, не предусмотренный стандартной процедурой, может оказаться попыткой похитить идентификационные данные и получить доступ к важной информации.

6.6.4 Обслуживание систем

Цель: Обеспечение целостности и доступности информационных сервисов.

6.6.4.1 Резервное копирование данных

Для важной информации, связанной с производственной деятельностью, а также для программного обеспечения должны регулярно создаваться и проверяться резервные копии.

Руководство по аудиту:

Резервное копирование – ключевой компонент для поддержания целостности и доступности информации. В организации должны быть предусмотрены подробные процедуры работ по резервному копированию и обращению с резервными копиями. В первую очередь необходимо проверить последовательность действий при резервном копировании: она должна соответствовать требованиям по производственной деятельности и безопасности и сочетаться с планами по восстановлению и обеспечению бесперебойной работы организации.

Для типичной сетевой конфигурации резервная копия включает в себя полную копию базовых данных, размещенных на сервере, плюс некоторое количество инкрементных обновлений, записываемых с заданной частотой в соответствии с требованиями по обеспечению целостности и доступности (например, ежедневно, еженедельно или ежемесячно). Удостоверьтесь, что копия охватывает всю область применения СУИБ.

Также важно проверить, каким образом маркируются резервные копии и где они хранятся; убедитесь, что каждую инвентарную единицу можно однозначно идентифицировать, данные о ней зарегистрированы надлежащим образом и обеспечены безопасные условия хранения. Хранилища носителей с резервными копиями и системы, с которых были получены эти данные, должны располагаться в разных местах; кроме того, должны быть реализованы средства управления, обеспечивающие для резервных копий тот же уровень безопасности, что и для исходных данных.

Установите, какие требования предъявляются к долгосрочному хранению критичных данных, как в организации проверяют соблюдение этих требований – носители, на которых записаны резервные копии, могут быть подвержены естественному износу и требовать замены. Также необходимо рассмотреть процедуры резервного копирования, какие коррекционные меры предусмотрены в случае невозможности создания копии, как организовано восстановление данных, как часто такое восстановление проводится, как регистрируются все проводимые мероприятия. Тестируется ли работоспособность носителей с резервными копиями? Тестовое восстановление данных из резервной копии не должно нарушать целостности информации; убедитесь, что данное требование надлежащим образом учтено. Проверьте, что требования по обеспечению бесперебойной работы организации соблюдаются в плане частоты, надежности носителей и доступности резервных копий.

6.6.4.2 Журналы действий операторов и регистрация ошибок

Обслуживающий персонал систем должен вести журналы своих действий. Журналы действий операторов должны подвергаться регулярным независимым проверкам.

Должны создаваться извещения об ошибках и предприниматься соответствующие корректирующие меры.

Руководство по аудиту:

В операционных процедурах по работе с компьютером должно указываться, какие журналы необходимо вести при работе в нормальном режиме и при сбоях. В рамках внутреннего мониторинга в журналах должны отражаться свидетельства анализа. При проверке журналов действий операторов в контексте работы организации необходимо выяснить, как в них отражены посменная работа, операции по передаче работы, особые требования и т.п. Также следует обратить внимание на помещение журналов (как генерируемых автоматически, так и создаваемых вручную) в архив: как журналы маркируются, каким образом можно получить к ним доступ.

Необходимо, чтобы по записям в журналах можно было проследить факт выполнения адекватных корректирующих действий по каждому сбою. В критерии анализа должна входить проверка на отсутствие нарушений безопасности; следует проверить, что это отражено в соответствующих процедурах и доведено до сведения руководства. Необходимо обеспечить адекватное разрешение всех ситуаций со сбоями. Кроме того, аудиторам следует проверить, что проведение любых коррекционных мероприятий возможно только при наличии соответствующих санкций.

6.6.5 Сетевое администрирование

Цель: Обеспечить защиту информации, передаваемой по сетям, и поддерживающей инфраструктуры.

6.6.5.1 Средства управления сетью

Для обеспечения безопасности информации, передаваемой по сетям, должен быть реализован ряд средств управления.

Руководство по аудиту:

Топология сети, а также среды функционирования, в особенности, когда речь идет о передаче важной информации, должны надлежащим образом планироваться и администрироваться; аудитор должен удостовериться в том, что у руководства имеются формальным образом подтверждающие это документы. Было ли уделено должное внимание ситуациям, когда внутренние сети имеют доступ к открытым сетям или используют их инфраструктуру, и реализованы ли соответствующие защитные механизмы?

В больших, сложных проектах могут потребоваться услуги специалистов-консультантов. Если консультанты не привлекаются, необходимо проверить уровень подготовки внутренних специалистов по развертыванию сетей. Определены ли наиболее уязвимые аспекты сетевых операций, и какие приняты защитные меры? Нарушения безопасности в сетях не всегда становятся очевидными немедленно; перехват данных, их копирование или модификация может производиться без очевидных следов.

Необходимо проверить, какие средства мониторинга используются для выявления подобных нарушений безопасности, и убедиться в том, что надлежащие действия описаны в процедурах уведомления об инцидентах. Сети, шифрование данных, цифровые подписи и т.п. – области, в которых технологии развиваются стремительно; нужно выяснить, как организация следит за новыми достижениями в данных областях и идентифицирует новые угрозы безопасности и соответствующие механизмы защиты по мере их появления.

6.6.6 Управление носителями информации и их защита

Цель: Предотвратить повреждение информационных ресурсов и приостановку работы организации.

6.6.6.1 Управление съемными носителями информации

Управление такими съемными носителями информации, как магнитные ленты, диски, кассеты и распечатанные отчеты, должно контролироваться.

Руководство по аудиту:

Выясните, как выносятся сменные носители информации за пределы территории организации. Вынос носителей может производиться для транспортировки в архив, для использования сотрудниками в рабочих целях и для уничтожения. В каждом из этих случаев должна быть предусмотрена соответствующая процедура и механизм регистрации. Такая процедура должна обеспечивать очистку сменных носителей от данных, чтобы гарантировать невозможность утечки информации. Если носитель подлежит уничтожению, или не будет в дальнейшем использоваться для хранения ценной информации по какой-либо другой причине, проверьте, как стерты хранившиеся на нем данные, что сделано с маркировкой, и т.д.

Также следует рассмотреть процедуры транспортировки для различных типов носителей: обеспечивают ли они достаточную степень защиты? Какие бы средства управления не использовались, контроль в данной области крайне затруднителен, поэтому необходимо проверить, учла ли этот момент организация при оценке рисков, и компенсируется ли это применением каких-либо дополнительных средств управления?

6.6.6.2 Уничтожение носителей информации

Уничтожение носителей информации, которые больше не нужны, должно осуществляться безопасным и надежным способом.

Руководство по аудиту:

Вопросы стирания информации на носителях, подлежащих уничтожению или альтернативному использованию уже рассматривались выше.

Выясните, каковы общие процедуры по уничтожению, используются ли услуги сторонних подрядчиков, удостоверьтесь, что организация выполнила необходимые проверки безопасности и проверки, предусмотренные другими

процессами, и что максимальный уровень конфиденциальности информации, который может быть задействован в таких процедурах, известен и подтвержден. Необходимо удостовериться, что какими бы ни были конкретные процедуры, в процессе уничтожения носителей не может произойти компрометации ценной информации, поскольку такая информация была стерта или уничтожена заранее. Для мероприятий по уничтожению должна быть предусмотрена, в том или ином виде, отчетность; убедитесь, что она предоставляет достаточную информацию для контрольного следа.

6.6.6.3 Процедуры оперирования информацией

Для защиты информации от несанкционированного раскрытия или использования должны быть разработаны процедуры по оперированию этой информацией и ее хранению.

Руководство по аудиту:

Аудиторам необходимо убедиться в наличии процедур по защите важной информации (вне зависимости от того, в какой форме она представлена), в соответствии со схемой классификации, принятой в организации. Как фиксируется в документах лицо, ответственное за информацию, каким образом получается разрешение на ее передачу?

В случаях, когда информацией оперируют неизвестные сотрудникам лица (такие, как курьеры), проводятся ли дополнительная проверка личности? Реализованы ли для них ограничения по доступу, и если да, то какие конкретно?

6.6.6.4 Защита системной документации

Системная документация должна быть защищена от несанкционированного доступа.

Руководство по аудиту:

Для ценной и конфиденциальной информации, такой как инструкция по эксплуатации системы, данные по настройкам и конфигурации, списки прав доступа и т.п., может потребоваться расширение стандартных процедур по работе с документацией. Такая системная документация может содержать важную и секретную информацию. Аудиторам необходимо удостовериться, что система классификации безопасности применяется к ним корректно и что документы надлежащим образом промаркированы.

Вполне вероятна ситуация, когда подобного рода документация предоставляется производителями, и, соответственно, устранение проблем будет основываться на основе данных, поступивших из стороннего источника. Выдача и распространение закрытых документов должно строжайшим образом контролироваться, там, где это возможно; в ряде случаев может потребоваться копирование. Если системная документация размещена на сетевом ресурсе, должны быть реализованы адекватные средства контроля доступа, разрешающие доступ к такой документации только уполномоченным сотрудникам.

6.6.7 Обмен информацией и программным обеспечением

Цель: Предотвратить потерю, модификацию или несанкционированное использование информации, которой обмениваются организации.

6.6.7.1 Соглашения об обмене информацией и программным обеспечением

Должны быть разработаны соглашения, некоторые из которых могут быть формальными, по обмену информацией и программным обеспечением (электронным способом или из рук в руки) между организациями.

Руководство по аудиту:

Аудиторам прежде всего следует установить, какие организации участвуют в обмене конфиденциальной информацией, а затем удостовериться, что существуют документы, устанавливающие контрактные обязательства. В данном контексте речь идет как об информации как таковой, так и о программном обеспечении. Такая ситуация может возникнуть, например, в случае, когда компания-производитель ПО разработала программы для оперирования критичными данными; организации может потребоваться обеспечить доступ к этому программному обеспечению через соглашения о депонировании у третьих сторон.

Рассмотрите, какую защиту предоставляют другие организации для информации, находящейся в их ведении.

6.6.7.2 Защита носителей информации при их транспортировке

Транспортируемые носители информации должны быть защищены от несанкционированного доступа, неправомочного использования или повреждения.

Руководство по аудиту:

Во всех случаях, когда происходит физическая транспортировка информации, необходимо задуматься, как осуществляется защита носителей, на которых размещена эта информация. Как организована транспортировка? Если с помощью курьерской службы, предоставляются ли защищенные, в том числе и от несанкционированного доступа, контейнеры? Данные могут передаваться сотрудниками на дисках или лентах, либо на переносных компьютерах; достаточно ли такой способ безопасен для передаваемых данных?

Кто определяет способ транспортировки, и какими критериями руководствуются эти лица? При использовании курьерской службы, вопрос о методах транспортировки может решаться самой службой, и вероятно использование транспортировки в стандартных условиях – достаточный ли уровень безопасности обеспечивается? Также следует рассмотреть вариант почтовой доставки, безопасен ли он? Во всех случаях, когда требуется транспортировка защищенной информации, должны быть предусмотрены процедуры, определяющие, как организуется доставка, должны быть четко

указаны необходимые разрешения на транспортировку, а их наличие зафиксировано документально.

6.6.7.3 Защита систем электронной коммерции

Системы электронной коммерции должны быть защищены от действий мошенников, возможности оспаривания действий и раскрытия или модификации информации.

Руководство по аудиту:

Аудиторам следует навести справки о текущих и будущих операциях организации с использованием электронной коммерции. Вся деятельность организации, связанная с электронной коммерцией, должна быть проанализирована в плане вопросов безопасности. Сюда входит проверка:

– наличия процесса авторизации: могут ли операции с использованием электронной коммерции проводиться только авторизованными сотрудниками организации;

– присутствия надлежащего разделения обязанностей: разделяются ли действия, которые в совокупности могут использоваться в мошеннических целях, и осуществляется ли контроль над ними;

– наличия соответствующих криптографических средств управления, позволяющих обеспечить аутентичность, целостность и конфиденциальность информации, обрабатываемой в связи с электронной транзакцией, а также существования политики, регулирующей применения таких средств управления;

– реализации соответствующих средств управления сетевой безопасностью, обеспечивающих защиту сети и сетевого узла организации, используемых для электронной коммерции, от атак, которые могут происходить из-за соединения с другими сетями;

– наличия достаточной защиты по рискам, исходящим извне;

6.6.7.4 Защита электронной почты

Для уменьшения риска нарушений безопасности, связанных с использованием электронной почты, должна быть разработана политика использования электронной почты и должны применяться необходимые меры контроля.

Руководство по аудиту:

На сегодняшний день обмен сообщениями по электронной почте широко распространен почти во всех организациях. Поскольку электронная почта крайне уязвима, необходимо тщательно изучить средства управления, применяемые для ее защиты: как контролируется информация, содержащаяся в тексте сообщения и в присоединенных файлах, как проверяется правильность доставки, как проверяется целостность и источник поступающих по электронной почте данных?

Если в организации применяются криптографические средства защиты, то какие именно? Проверяется ли информация, пришедшая по электронной

почте, на наличие вирусов перед использованием? Имеют ли сообщения электронной почты, рассылаемые внутри организации, особый статус целостности в отличие от сообщений, отправляемых внешним адресатам? Если да, то каким образом он определяется и отслеживается?

Использование электронной почты связано со значительным риском судебных разбирательств, и в организации должна иметься четко сформулированная и реализованная политика на данный счет. Внутренние сообщения могут быть непреднамеренно отправлены внешним адресатам, присутствует риск ненамеренного принятия на себя контрактных обязательств, сообщения и прикрепленные файлы могут сохраняться в резервных копиях годами. Стандартные формулировки отказа от ответственности, включаемые в текст сообщений, могут помочь, однако их правовой статус в качестве средства защиты представляется сомнительным.

Аудиторам следует удостовериться, особенно в случаях, когда разрешена отправка электронной корреспонденции на внешние адреса, что организацией была проведена соответствующая оценка рисков и ее результаты были учтены. Например, в качестве меры защиты может быть введено ограничение, позволяющее пользоваться электронной почтой только узкому кругу сотрудников. Если такое ограничение присутствует, то как обеспечивается его выполнение? Протестируйте использованный механизм защиты.

6.6.7.5 Защита систем электронного офиса

Для контроля риска, которому подвергаются производственные процессы и система безопасности в связи с использованием систем электронного офиса, должны быть подготовлены и реализованы соответствующие политики и рекомендации.

Руководство по аудиту:

Хотя использование систем электронного офиса может давать существенный прирост производительности, вместе с этим возрастает и риск неправомерного использования, раскрытия или уничтожения обрабатываемой информации в результате плохо продуманных процедур работы. Аудиторам необходимо определить, какие процедуры были разработаны, как они были реализованы, какую информацию и где необходимо хранить, и определены ли где-нибудь сопутствующие риски.

Использование электронных систем планирования дел может привести к распространению закрытой информации и данных о перемещениях ключевых фигур в руководстве среди лиц, для которых эта информация не предназначена; базы данных по персоналу с общим доступом могут содержать конфиденциальную личную информацию; пакеты управления документооборотом могут основывать свою работу на данных, которые были повреждены либо опущены при вводе, или вносились недостаточно

компетентными или не имеющими соответствующего разрешения сотрудниками.

Проанализируйте контроль доступа к этим системам и пересылаемой информации. Знают ли пользователи о том, что к информации, которую они передают, может легко получить доступ любое лицо, имеющее доступ к офисной системе?

В случаях, когда разрешен доступ к средствам электронного офиса извне (например, в случае надомной работы сотрудников, или взаимодействия с другими организациями), внешние соединения могут существенно понизить уровень безопасности сети в целом, и необходимо рассмотреть возможность использования дополнительных средств управления. Еще большую важность этот вопрос приобретает при соединении через сети с открытым доступом, такие, как Интернет.

6.6.7.6 Общедоступные системы

Помещение информации в открытый доступ должно быть санкционировано в рамках формальной процедуры, и целостность этой информации должна быть защищена для предотвращения несанкционированной модификации.

Руководство по аудиту:

Если для публикации информации, а также для получения информации и данных в организации используются системы с открытым доступом, такие, как Web-сервер, подключенный к сети Интернет, аудиторам необходимо выяснить, какие средства управления используются для защиты безопасности, и проверить, что они реализованы корректно.

Сюда входит проверка процесса утверждения, необходимого для публикации информации. Могут ли сотрудники добавлять новые Web-страницы или изменять уже опубликованные без получения соответствующего разрешения? Существует ли в организации сотрудник, в чьи обязанности входит регулярная проверка содержания опубликованной информации? Проверял ли кто-либо из сотрудников информацию, опубликованную или полученную с помощью систем с открытым доступом на соответствие нормам действующего законодательства, особенно, законодательства той страны, где информация была помещена в открытый доступ? Защищена ли опубликованная информация от возможности манипуляций извне?

Помимо обеспечения защиты опубликованной информации, может потребоваться защита корпоративной сети от вторжений, использующих соединение, необходимое для публикации, в целях получения несанкционированного доступа. Аудиторам необходимо проверить, что для защиты от такого несанкционированного доступа реализованы средства управления.

6.6.7.7 Другие формы информационного обмена

Должны существовать политики, процедуры и средства управления, обеспечивающие защиту информационного обмена, осуществляемого с помощью средств голосовой связи, факсимильной связи и видеоконференций.

Руководство по аудиту:

Данное средство управления относится к обеспечению безопасности при использовании мобильных вычислительных устройств, стационарных и мобильных телефонов, факсимильных аппаратов, карманных компьютеров, автоответчиков, и т.п. Аудиторам необходимо выяснить, какие процедуры разработаны для управления данным видом информационного обмена, и проверить их соответствие средствам управления.

Необходимо убедиться, что сотрудники проинформированы относительно данных процедур. Это можно сделать, например, расспросив их о том, как они пользуются мобильными телефонами, автоответчиками или факсовыми аппаратами, и выяснить, осведомлены ли они о связанных с таким использованием рисках.

6.7 Управление доступом

6.7.1 Производственные требования к управлению доступом

Цель: Управление доступом к информации.

6.7.1.1 Политика управления доступом

Производственные требования к управлению доступом должны быть определены и задокументированы, доступ к системам должен ограничиваться в соответствии с политикой управления доступом.

Руководство по аудиту:

Аудиторам необходимо обеспечить четкое определение прав доступа в документе, определяющем политику контроля доступа, и убедиться в наличии реализованных механизмов по обеспечению требований этой политики. Любой доступ к конфиденциальной информации должен основываться на принципе необходимости: разрешение на доступ должно выдаваться в соответствии с производственными требованиями и при наличии необходимости в данной информации для выполнения работы.

Аудиторы должны быть готовы к выяснению причин, по которым сотрудники (в ряде случаев – из числа высшего руководства организации) имеют доступ к определенной информации, если соблюдение принципа необходимости неочевидно. Проверьте также, что доступ к важной и конфиденциальной информации производится в соответствии с классификацией защиты, и что сотрудники, имеющие доступ к такой информации, соответствующим образом проинструктированы. Неконтролируемое использование конфиденциальной информации

неквалифицированными сотрудниками может привести к катастрофическим последствиям.

6.7.2 Управление доступом пользователей

Цель: Обеспечить надлежащее утверждение, назначение и поддержку прав доступа.

6.7.2.1 Регистрация пользователей

Для управления доступа ко всем многопользовательским информационным системам и сервисам должна существовать формальная процедура регистрации пользователей и удаления учетных записей пользователей.

Руководство по аудиту:

Необходимо обеспечить формальный контроль и регистрацию доступа пользователей. В соответствии с политиками, как это рассматривалось выше, аудиторы должны гарантировать, что уровни доступа всех пользователей базируются на формальном процессе регистрации и авторизации, а факты доступа регистрируются. Проверьте, что такие регистрационные записи соответствуют действительности; удалены ли сотрудники, ушедшие с работы или получившие другие обязанности из соответствующих списков?

В большинстве случаев аудиторам придется уделить значительное количество времени работе с системными администраторами для изучения настроек операционной системы, определяющих права доступа для конкретных групп и отдельных пользователей с целью убедиться, что доступ разрешен исключительно для зарегистрированных и прошедших соответствующую авторизацию пользователей.

6.7.2.2 Управление привилегиями

Предоставление и использование привилегий должно ограничиваться и контролироваться.

Руководство по аудиту:

По определению, особые привилегии предоставляют доступ к системным функциям, использование которых в обычной ситуации ограничено. Обратите особое внимание на системных администраторов, системных инженеров и инженеров поставщика оборудования или программного обеспечения, а также на всех тех сотрудников, чьи должности подразумевают привилегированный доступ к системам. Убедитесь, что хотя данный уровень доступа должен быть ограничен, в то же время средства привилегированного доступа в каждый момент времени имеются более чем у одного сотрудника, поскольку без соответствующего мониторинга доступность и возможность контроля над производимыми действиями может пострадать.

Доступ к защищенной информации может также включать коды сейфовых замков и других защищенных областей; такие коды также должны соответствующим образом регистрироваться и периодически сменяться.

Снова необходимо убедиться, что доступность информации не пострадает из-за того, что права на доступ имеются только у одного сотрудника. Также следует проверить, что привилегии предоставляются в соответствии с принципом необходимости и по каждому конкретному случаю, аннулируются, как только в них отпадает необходимость, и ассоциированы с выделенной учетной записью, не используемой в рамках нормальной трудовой деятельности.

6.7.2.3 Управление паролями пользователей

Назначение паролей должно контролироваться посредством формального процесса управления.

Руководство по аудиту:

Контроль паролей тесно связан с вопросами привилегированного доступа; это основной (хотя и не единственный) механизм обеспечения доступа к ресурсам для авторизованных пользователей. Узнайте, как назначаются и контролируются пароли: иногда этот вопрос решается самим пользователем, в других случаях пароли создаются и назначаются системным администратором. Если назначение паролей централизованно, где хранятся пароли, обеспечена ли защита безопасности, кто имеет доступ к хранилищу паролей? Каким бы ни был процесс назначения паролей, он должен основываться на принципе однозначной идентификации пользователя, и предусматривать формальную процедуру, требующую от пользователей смены первичного, временного пароля, на постоянный. Проверьте, что пользователи подписали обязательства по сохранению конфиденциальности пароля, и что они осознают ответственность за их выполнение.

6.7.2.4 Пересмотр прав доступа пользователей

Руководство должно регулярно выполнять формальный процесс пересмотра прав доступа пользователей.

Руководство по аудиту:

Простое назначение прав доступа, без регулярного их пересмотра и обновления, недостаточно для обеспечения безопасности. Аудиторам необходимо убедиться в наличии и применении процедур по регулярному пересмотру всех видов прав доступа для пользователей. Эти процедуры могут включать формальный аудит для проверки соответствия, за которым следует пересмотр прав доступа со стороны руководства для проверки совместимости с производственными требованиями и требованиями политики безопасности.

Важно обеспечить, чтобы при изменении ситуации, увольнении и наборе сотрудников, изменении должностных обязанностей, развитии систем, права доступа отдельных пользователей должным образом контролировались, и соответствовали новым требованиям. Удостоверьтесь, что для особых привилегий предусмотрены дополнительные меры контроля (например, внеплановые или точечные проверки).

6.7.3 Обязанности пользователей

Цель: Предотвратить несанкционированный доступ пользователей.

6.7.3.1 Использование паролей

При выборе и использовании паролей пользователи должны следовать установленным процедурам поддержания режима безопасности.

Руководство по аудиту:

Проверьте, что политика по смене паролей (в плане частоты смены, минимальной длины и состава пароля) соответствует требованиям организации и информационным требованиям по защите безопасности. В некоторых системах правила назначения паролей обязательно предусмотрены, в других они отсутствуют – проверьте, какие дополнительные меры реализованы, если система автоматически не применяет такие правила. При необходимости, попросите сотрудников продемонстрировать, как они меняют собственный пароль – знакомы ли они с критериями выбора пароля, соответствуют ли используемые ими коды политике, принятой в организации?

Также проверьте, не записаны ли пароли в легкодоступных местах (в блокнотах, на наклейках, прикрепленных к монитору, и т.п.). Дополнительные сведения можно получить в разделе «Управление паролями пользователей» выше, а также в других разделах, на которые присутствуют ссылки по тексту. При проверке использования паролей в организации, аудиторам следует заручиться соответствующим разрешением руководства.

6.7.3.2 Пользовательское оборудование, оставленное без присмотра

Пользователи должны обеспечить надлежащую защиту оборудования, оставляемого без присмотра.

Руководство по аудиту:

С точки зрения аудита, главное здесь – наличие процедур, проверка того, что сотрудники в курсе требований и возможных опасностей, а также обеспечение выполнения принятых процедур. Проверьте, нет ли в организации оставленных без присмотра терминалов, не выключенных и незащищенных паролем. Хранители экрана на персональных компьютерах также должны быть защищены паролем – проверьте выполнение этого требования. Попросите включить любой из выключенных терминалов – информация должна быть недоступна.

Оборудование с повышенными требованиями к безопасности, такое, как сетевые серверы, коммуникационное оборудование и т.п., которое штатно работает в автономном режиме, должно размещаться в защищенных местах – убедитесь, что это так, и что обеспечены достаточные меры защиты.

6.7.4 Управление доступом к сети

Цель: Обеспечить защиту сетевых сервисов.

6.7.4.1 Политика использования сетевых сервисов

Пользователи должны получать прямой доступ только к тем сервисам, использование которых им явным образом разрешено.

Руководство по аудиту:

Пользователь, заходящий на терминал или в приложение должен иметь доступ только к той информации и сервисам, которые необходимы для выполнения его должностных обязанностей, и использование которых ему разрешено. В качестве примера можно привести приложение для доступа к базе данных, в котором пользователь терминала может просмотреть личные данные по прохождению тренинга, но не имеет доступа к данным по заработной плате, хранящимся в той же базе данных. К чему конкретно имеет доступ тот или иной пользователь должно быть четко определено: для некоторых приложений полный доступ ко всей информации может не представлять проблемы, в то время как для других приложений такая ситуация критична. Возможно, что доступ требуется ограничить не только из соображений конфиденциальности; речь может идти о риске нарушения целостности информации, или опосредованной компрометации других данных при использовании определенной информации.

Аудитору необходимо убедиться, что требуемые ограничения идентифицированы и реализованы в соответствии с политикой контроля доступа, что о наличии ограничений упомянуто в руководствах, что права доступа включены в дизайн или настройки приложения, и, наконец, что примененные средства эффективны. Исследуйте также доступ на уровне операционной системы, в ситуации, когда сотрудник подключается с терминала к основному серверу или вычислительному узлу: какой доступ разрешен к структуре директорий, операционным настройкам, и так далее?

6.7.4.2 Принудительная маршрутизация

Путь от пользовательского терминала к сервису на компьютере должен контролироваться.

Руководство по аудиту:

Там, где в организации используется политика принудительная маршрутизация (приведенная в соответствие с политикой контроля доступа – см. выше), выясните, как она реализована технически, и удостоверьтесь, что отсутствуют способы ее обойти. Гибкие правила сетевой маршрутизации могут позволять отдельным пользователям использовать для подключения любой терминал (для менее защищенных зон это может противоречить политике безопасности); сообщения могут маршрутизироваться через альтернативные сетевые мосты; телефонные линии и другие внешние подключения могут изменяться в периоды нехватки емкости и на время проведения ремонтных работ.

Организация должна иметь возможность представить подробный план топологии сети и пояснить, какие средства управления были использованы

для реализации принудительной маршрутизации. Проверьте, что примененные средства управления действительно реализуют необходимые ограничения.

6.7.4.3 Аутентификация пользователей при внешних подключениях и аутентификация узлов сети

Должна осуществляться аутентификация удаленных пользователей.

Подключения к удаленным компьютерным системам должны аутентифицироваться.

Руководство по аудиту:

Любая организация, эксплуатирующая защищенные системы, допускающие доступ извне или удаленные соединения, должна выполнить требования данного средства управления в полном объеме. Аудиторам необходимо проверить, что идентифицированы все порты, и проведена полная оценка рисков.

Начать следует с выяснения, на каком уровне проводится аутентификация – на уровне конкретных приложений или на уровне сетевой операционной системы. Если на уровне приложений, то проводились ли оценки или тесты, позволяющие понять, не аннулирует ли такую аутентификацию проникновение на уровне операционной системы? Адекватны ли реально примененные механизмы аутентификации важности защищаемой информации? Удостоверьтесь, что руководство полностью осведомлено о рисках и уделило должное внимание рассмотрению необходимых средств управления, а выбранные средства управления были корректно реализованы и регулярно проверяются.

Существует множество механизмов аутентификации; удостоверьтесь, что выбранный механизм (или механизмы) соответствует требованиям по обеспечению безопасности. Если используются средства прямого коммутируемого доступа, выясните, как они работают; одним из возможных подходов для проверки идентификации удаленного узла является операция ответного звонка, однако могут потребоваться более надежные методы аутентификации, например, с использованием токенов.

6.7.4.5 Сегментация сетей

В сетях должны быть реализованы средства управления для выделения групп информационных сервисов, пользователей и информационных систем.

Руководство по аудиту:

Чем больше домен, тем труднее обеспечить его защиту. Это соображение верно для сетей в той же степени, что и для любых других структур. Очень вероятно, что из защищенных сетей потребуется обеспечить доступ к более широким аспектам производственных операций – электронной почте, интранет-страницам, сетям других организаций и т.п.; в связи с этим требуется отделение особо важных зон.

Необходимая степень разделения сетевых ресурсов может быть достигнута физическим разделением сети на сегменты, либо путем

реализации средств управления сетевыми соединениями и маршрутизацией, например, посредством мостов, маршрутизаторов, межсетевых экранов и т.д.

Аудитору требуется установить состав доменов безопасности, выяснить, соответствуют ли они требованиям по обеспечению безопасности, как они определены и интегрированы в структуру сетевых операций. Следует также учесть тот факт, что использование доменов безопасности может ограничить операционную производительность, поэтому необходимо удостовериться, что в связи с этим не было допущено никаких компромиссов в плане обеспечения безопасности защищенных зон.

6.7.4.6 Управление сетевыми подключениями и управление сетевой маршрутизацией

Возможности подключения пользователей к коллективно используемым сетям должны ограничиваться в соответствии с политикой управления доступом.

В совместно используемых сетях должны использоваться средства контроля маршрутизации, чтобы подключения компьютерных систем и информационные потоки не нарушали политику управления доступом к производственным приложениям.

Руководство по аудиту:

В случае совместного использования сетей может возникнуть необходимость ограничить возможности пользователей по установлению соединений, в соответствии с политикой контроля доступа. Если пользователи или сервисы будут находиться за пределами физически защищенной области и использовать межсетевые соединения, возможно, на базе транспорта с открытым доступом, аудиторам следует выяснить, разрешен ли доступ такого рода к приложениям и системам, а если да, то накладываются ли на него дополнительные ограничения по сравнению с доступом внутренних пользователей и сервисов. Если ограничения на доступ к сервисам на накладываются на уровне приложений, то какова вероятность того, что будет использоваться средство сетевого управления, отличное от применяемого локально, каким образом это реализовано, и соответствует ли реализация политике?

Принудительная маршрутизация между удаленными сетями может основываться на сторонних поставщиках; если такая ситуация существует, какие гарантии имеет организация относительно целостности и доступности маршрута, и как обеспечивается непрерывность его использования? Что происходит, когда ремонтные работы или аварии вынуждают организацию использовать другие маршруты? При прохождении через сети с открытым доступом невозможно обеспечить фиксированный маршрут; принят ли этот факт во внимание, и какие альтернативные транспортные механизмы используются?

6.7.4.7 Защита сетевых сервисов

Должно быть предоставлено четкое описание атрибутов безопасности всех сервисов, используемых в организации.

Руководство по внедрению:

Подключение к сетевым сервисам, предоставляемым сторонними организациями, ведет к уязвимости в плане попыток несанкционированного доступа со стороны третьих лиц, что приводит к нарушениям конфиденциальности и потере целостности. Особое внимание следует также уделить доступности, проверив способность к восстановлению нормального функционирования сервисов поставщика после сбоев на линии или поломки оборудования. Обеспечьте соблюдение стандартов безопасности на время восстановительных работ поставщика. Необходимо учесть подробности мер по обеспечению безопасности при проведении оценки рисков. При определенных обстоятельствах может потребоваться использование дополнительных средств управления для компенсации обнаруженных слабых мест в защите.

Руководство по аудиту:

В случае, когда организация полагается на сторонних поставщиков сетевых услуг, крайне важно иметь максимально полную информацию обо всех соответствующих аспектах безопасности. Проверьте, что организация получила такую информацию, что она зафиксирована документально, что атрибуты безопасности достаточны и соответствуют потребностям организации, что полученная информация учтена в операционных процедурах и средствах управления безопасностью, и что она регулярно пересматривается и проверяется. Запомните, что указанные средства управления должны охватывать все аспекты обеспечения конфиденциальности, целостности и доступности.

6.7.5 Управление доступом к компьютерам

Цель: Предотвратить несанкционированный доступ к компьютерам.

6.7.5.1 Автоматическая идентификация терминалов и процедуры входа в систему с терминала

Для аутентификации подключений к конкретным узлам сети должна использоваться автоматическая идентификация терминалов.

Доступ к информационным сервисам должен осуществляться с помощью надежной процедуры входа в системы.

Руководство по аудиту:

Для определенных местонахождений и при использовании портативного оборудования для аутентификации систем может применяться автоматическая идентификация терминала; доступ может санкционироваться только после успешной аутентификации. Если используется подобная схема, установите, как выполняется проверка аутентификации, что происходит, когда на терминале обнаруживается сбой и необходима его замена? Какие

еще средства защиты применяются, если все же требуется идентификация пользователя в той или иной форме, зафиксирован ли терминал физически, или он расположен в защищенной зоне?

Процедуры регистрации в системе могут быть существенно шире, чем простой ввод правильного имени пользователя и пароля. Требуется ли от пользователя проведение серии действий для регистрации, что происходит при вводе неправильной информации, есть ли период задержки, предусмотрена ли блокировка системы после нескольких неудачных попыток регистрации? Если да, то каков механизм возврата из данной ситуации?

Иногда приложение не может обеспечить достаточного уровня защиты при регистрации – например, в случае, когда не ограничивается число неуспешных попыток. В этом случае следует проверить, вводятся ли дополнительные средства управления (например, посредством физического ограничения доступа к терминалу). При проведении оценки рисков должны были учитываться каждая система и приложение, методы доступа, а также их адекватность – проверьте, так ли это.

6.7.5.2 Идентификация и аутентификация пользователей

Всем пользователям должны быть присвоены уникальные идентификаторы (ИД пользователя), которые будут использоваться только этими пользователями, с целью обеспечить возможность отслеживания действий отдельных лиц. Для подтверждения заявленной аутентификационной информации пользователя должен быть выбран подходящий метод аутентификации.

Руководство по аудиту:

Термин «пользователь» должен охватывать всех лиц, использующих средства и системы обработки информации, включая системных администраторов, менеджеров и пользователей приложений. Проверьте, используются ли уникальные идентификаторы пользователей, или допускается совместное использование идентификаторов. Если идентификатор может использоваться несколькими пользователями, выясните, почему это необходимо, каким образом производится контроль, и какие требуются разрешения? Для критичных функций, таких как администрирование системы, должен присутствовать идентификатор пользователя, выделенный исключительно для данных целей, а также должна проводиться регистрация времени и лица, инициирующего то или иное событие. Выясните, для каких ситуаций требуется ведение таких регистрационных журналов, в течение какого срока они хранятся, возможна ли их модификация, когда и при каких обстоятельствах они просматриваются? Если в конкретном приложении не предусмотрена возможность отслеживания подобной информации, определите, какие другие средства управления применяются.

Необходимо определить, обеспечивают ли используемые в организации процедуры аутентификации достаточный уровень безопасности для информации, систем и приложений, которые необходимо защитить? Использование паролей обычно считается недостаточным методом защиты для областей высокого риска. Для определения надлежащих процедур идентификации и аутентификации пользователей в этом случае необходимо проведение оценки рисков.

6.7.5.3 Система управления паролями

Системы управления паролями должны предоставлять эффективное, интерактивное средство обеспечения надежных паролей.

Руководство по аудиту:

В организации должна присутствовать некая общая политика по использованию паролей. Любые дополнительные требования для особо важных областей должны быть, по возможности, приведены в соответствие с этой политикой и оформлены в виде дополнений к ней. Аспекты, которые необходимо проверить аудиторам включают:

– длину и состав паролей;

– частоту смены паролей;

– использование паролей, совпадающих для различных пользователей и приложений;

– безопасность при оперировании паролями и их хранении;

– смена паролей по умолчанию.

Помимо прочего, необходимо проанализировать процесс смены паролей: как и где он регистрируется, предусмотрен ли запрет на использование старых паролей, требует ли приложение подтверждения нового пароля перед его принятием (например, путем повторного ввода). При необходимости, попросите пользователей продемонстрировать процедуру смены пароля.

6.7.5.4 Использование системных утилит

Использование системных программ-утилит должно ограничиваться и строго контролироваться.

Руководство по аудиту:

Некоторые утилиты позволяют получить доступ к частям системы, недоступным для приложений, и могут также обеспечивать обход системных средств управления. Аудиторам прежде всего необходимо установить, что организация обеспечивает общий контроль над установленными утилитами, проверить, что список утилит известен и их использование разрешено, и что при работе с ними применяется соответствующий контроль и ограничения доступа. Проверьте, что на отдельных системах не установлены дополнительные или модифицированные утилиты.

В организациях со слабо регулируемой системой безопасности могут быть установлены условно-бесплатные утилиты, использование которых

может нанести ущерб не только конфиденциальности информации, но и ее целостности и доступности. Проверьте также, что в памяти систем не осталось забытых резидентных утилит, подлежащих удалению. И, наконец, проверьте, что никто, кроме лиц, получивших соответствующее разрешение, не может получить доступ к системным утилитам и использовать их.

6.7.5.5 Сигнал тревоги, предупреждающий о принуждении, для защиты пользователей

Пользователям, которые могут стать объектом для принуждения, должна быть предоставлена возможность использовать сигнал тревоги, предупреждающий о принуждении.

Руководство по аудиту:

Там, где организация идентифицировала необходимость использования сигнала тревоги о принуждении, аудитору прежде всего следует установить, все ли необходимые требования соблюдены: например, все ли возможные точки охвачены, раздается ли сигнал тревоги в нужных местах, можно ли отключить сигнал?

Активация сигнала тревоги должна быть простой, но не настолько, чтобы приводить к ложным сигналам. Сигнал тревоги может активироваться физически, например, нажатием кнопки, или вводом специального кода при работе с приложением. Для некоторых сигналов тревоги должен быть предусмотрен незаметный способ активации, чтобы не подвергать персонал лишней опасности.

Рассмотрите процедуры реагирования на сигналы тревоги, обязанности и действия, которые должны быть обозначены особо. Первоначальные действия при реакции на тревогу должны быть простыми для понимания и, при необходимости, выполняться немедленно; здесь аудитору следует проверить, что соответствующий персонал знает, что необходимо делать, не прибегая к чтению инструкций, по крайней мере, для самых первых шагов, предусмотренных процедурой реагирования.

6.7.5.6 Блокировка терминала по времени и ограничение времени подключения

Для предотвращения доступа незарегистрированных пользователей к бездействующим терминалам, находящимся в зонах повышенного риска или обслуживающим системы повышенного риска, должно производиться отключение этих терминалов по истечении заданного периода бездействия.

Для дополнительной защиты приложений повышенного риска должны использоваться ограничения на время подключения.

Руководство по аудиту:

Возможность отключения определенных терминалов по бездействию по истечении определенного периода должна рассматриваться в любых ситуациях, когда возможен открытый доступ или доступ персонала, безопасность которого проверена в меньшей степени. Выясните, где

определены соответствующие меры, и определите, достаточны ли выбранные периоды с точки зрения уровня доступа, уязвимости и операционных требований. Узнайте, на чем основано определение работы/бездействия, на определенном использовании приложения или просто на перемещениях мыши. Проверьте, что отключение по периоду бездействия последовательно применяется во всех местах высокого риска – в некоторых офисных помещениях с открытым доступом может находиться несколько терминалов, требующих такого способа защиты – и проверьте, что данная схема везде работоспособна. Там, где отключение по периоду бездействия основано на функциях операционной системы, таких, как хранитель экрана Windows, проверьте, что нужная функция не отключена, и, конечно же, убедитесь в том, что использование пароля производится в соответствии с принятой политикой.

В некоторых приложениях помимо блокировки по периоду бездействия могут использоваться ограничения по времени подключения. Ограничения по соединению должны применяться в приложениях, подверженных высокой степени риска. Снова требуется выяснить, где применяется данный метод, проверить, что его использование соответствует требованиям, и что таймеры нельзя обойти, например, оставив какую-либо транзакцию в незавершенном состоянии.

6.7.6 Управление доступом к приложениям

Цель: Предотвратить несанкционированный доступ к информации, хранимой в информационных системах.

6.7.6.1 Ограничение доступа к информации

Доступ к информации и функциям прикладных систем должен ограничиваться в соответствии с политикой управления доступом.

Руководство по аудиту:

Аудиторам следует прежде всего удостовериться, что доступ к информации, предоставляемой отдельными приложениями, соответствует производственным требованиям и происходит в соответствии с политикой контроля доступа. Например, доступ к одной и той же базе данных может осуществляться из различных приложений; можно ли получить доступ к конфиденциальной информации, недоступной из одного приложения, с помощью другого?

Во многих случаях пользователям следует знать об информации или функциях приложений, использование которых для них не разрешено; соответственно, следует избегать показа пунктов меню, недоступных по соображениям безопасности. То же самое относится и к руководствам пользователей по конкретным приложениям. Обратите особое внимание на редко используемые компоненты приложений, такие как сопроводительные утилиты: осуществляется ли достаточный контроль по работе с ними?

Также следует выяснить, что происходит с доступной информацией: разрешены ли пользователям чтение, запись, есть ли в этом необходимость, накладываются ли ограничения на вывод информации? Печать в сетевых системах может выполняться на устройствах совместного доступа, физически удаленных от оператора, – каким образом осуществляется контроль в этом случае? Необходимо обеспечить соответствие системе классификации безопасности при защите информации.

6.7.6.2 Изоляция уязвимых систем

Уязвимые системы должны иметь выделенную (изолированную) вычислительную среду.

Руководство по аудиту:

Там, где речь идет об оперировании информацией с высокой степенью уязвимости, может возникнуть необходимость реализовать на том или ином уровне изоляцию. Такие области должны идентифицироваться организацией, которая должна при этом принять во внимание вопросы безопасности, доступности и операционные вопросы. Система может иметь настолько высокие требования по безопасности, что будет необходима полная ее изоляция, либо, в качестве альтернативного варианта, реализация связей с другими системами через выделенный защищенный порт.

Кроме обычных процедур и определений, убедитесь, что такие системы идентифицированы в рамках оценки рисков, а необходимость их изоляции достаточно подтверждена – жесткий контроль доступа (как в случае изоляции) может противоречить с производственными требованиями по использованию системы; проверьте, что между этими двумя моментами достигнут нужный компромисс. Если требуется выделение отдельной системы, рассмотрите предусмотренные меры по восстановлению работоспособности после сбоя, какие ограничения накладываются на ввод данных или загрузку программ с носителей информации, и какие создаются резервные копии.

6.7.7 Мониторинг доступа

Цель: Выявить несанкционированные действия.

6.7.7.1 Регистрация событий

Все исключительные ситуации и другие события, связанные с нарушением безопасности, должны регистрироваться в контрольном журнале. Записи в таком журнале должны храниться в течение заданного промежутка времени с целью их последующего использования для расследований и для проверки выполнения политики управления доступом.

Руководство по аудиту:

Для всех систем, в которых выполняется обработка информации, должен вестись в той или иной форме журнал, независимый от пользователя и недоступный ему. Аудиторам следует определить области, в которых такой

подход соответствует требованиям по безопасности, и изучить его реализацию в организации. Удостоверьтесь, что все записи, которые требуется сохранять в течение определенного времени согласно политике хранения записей или в целях сбора свидетельств, должным образом помещаются в архив. Что именно регистрируется в журналах? Как минимум, там должна содержаться информация о событии, лице, инициировавшем это событие, выполненные изменения (там, где это применимо), дата и время. Дополнительно может потребоваться регистрация кодов транзакций и идентификатор терминала. Определите, что считается событием, и удостоверьтесь, что учтены все исключения. Выясните, как долго требуется хранить зарегистрированную информацию, в каком виде, и с использованием каких средств защиты; проверьте, что требования соблюдаются. В качестве примера событий можно привести внесение изменений системными администраторами, а также неудачные попытки входа в систему или осуществления доступа к данным.

6.7.7.2 Мониторинг использования системы

Должны быть определены процедуры мониторинга использования средств обработки информации, и результаты мониторинга должны регулярно анализироваться.

Руководство по аудиту:

Мониторинг включает в себя проверку журналов событий безопасности на наличие признаков непредусмотренных действий. Выполненная оценка рисков должна указывать, где и какой мониторинг следует вести. В качестве примеров можно привести:

– неудачные попытки доступа;

– необычные значения данных;

– попытки внесения изменений в защищенные данные;

– чрезмерное использование определенных данных;

– доступ под редко используемым или избыточным идентификатором пользователя.

Так же, как и выше, необходимо проверить, как ведется работа с записями, и удостовериться, что их модификация или удаление невозможны. Аудиторам следует установить, какие меры предприняты организацией для обеспечения разделения обязанностей в плане деятельности по анализу действий и самих действий, подлежащих анализу, с целью гарантировать правильность результатов.

Необходимо также проверить, насколько часто изучаются журналы регистрации – чем выше соответствующий уровень риска в отношении безопасности, тем чаще необходимо просматривать журналы. Такая проверка должна проводиться также для обеспечения надлежащей эффективности и производительности в процессе анализа данных журналов.

Журналы, генерируемые системой или процессом регистрации событий, зачастую могут достигать больших объемов. Соответственно, это может привести к тому, что важная для аудита информация по инцидентам безопасности затеряется среди менее важных данных. Таким образом, необходимо использовать средства фильтрации журналов аудита, с использованием правил фильтрации, обеспечивающие отбор всех требуемых инцидентов и действий. Аудитору следует расспросить сотрудников организации о наличии и использовании таких средств, и выяснить, как они применяются для обнаружения инцидентов и реагирования на них.

6.7.7.3 Синхронизация системных часов

Для обеспечения точности контрольных журналов системные часы компьютеров должны быть синхронизированы.

Руководство по аудиту:

Без синхронизации времени на всех системах, регистрация событий может быть неточной, а значит, скомпрометированной. Организации необходимо установить базу для отсчета времени; для большинства случаев это будет местное время, однако для международных организаций может потребоваться использование другой базы, например, времени по Гринвичу (GMT). Также должно быть предусмотрено средство мониторинга системных часов, позволяющее, при необходимости, производить корректировку времени.

Выясните, как производится перевод часов с летнего времени на зимнее. Производятся ли какие-либо дополнительные проверки при подключении к сети портативных систем? Регистрация событий опирается на точность системных часов, перевод времени может использоваться для фальсификации записей; проверьте наличие ограничений по доступу к системным часам. Не забудьте также о настенных часах, которые могут использоваться при необходимости регистрации событий вручную, например, при доставке грузов и уведомлении об инцидентах.

6.7.8 Мобильные вычисления и дистанционная работа

Цель: Обеспечить безопасность информации при использовании средств мобильных вычислений и дистанционной работы.

6.7.8.1 Мобильные вычисления

Должна существовать формальная политика и должны быть выбраны соответствующие средства управления для защиты от рисков, связанных с работой со средствами мобильных вычислений, особенно в незащищенной среде функционирования.

Руководство по аудиту:

Организация должна идентифицировать факты использования любых мобильных вычислительных устройств; сюда входит использование мобильных телефонов, лэптопов, ноутбуков и карманных компьютеров за

пределами организации (например, дома, на территории заказчика, в отелях или местах проведения конференций), а также любые удаленные подключения к внутренним средствам обработки информации в организации с использованием таких устройств. Поскольку использование подобных устройств и оборудования весьма распространено, а мобильные вычисления происходят за пределами организации, прямой аудит такого использования обычно затруднен.

В связи с этим, особенно важно внимательно проанализировать средства управления, правила и процедуры, реализованные в организации для обеспечения безопасного использования подобных мобильных устройств. Сюда входят, в частности, средства управления, которые должны быть реализованы для физической защиты таких устройств.

Также необходимо произвести проверку того, что все указанные выше средства управления реализованы корректно. При проверке средств управления необходимо также установить, как в соответствующей политике обозначены вопросы защиты паролей и защиты от вирусов в применении к мобильным компьютерам? Убедитесь, что имеются в наличии средства управления, достаточные для защиты удаленного доступа, а там, где это требуется, применяются средства криптографической защиты.

6.7.8.2 Дистанционная работа

Должны быть разработаны политики, процедуры и стандарты для разрешения и контроля дистанционной работы.

Руководство по аудиту:

Дистанционная работа должна разрешаться только при наличии и реализации достаточных средств управления, включая средства физической защиты, управления контролем доступа, и обеспечения безопасности удаленного соединения. Используемое дома оборудование должно быть включено в инвентарную опись ресурсов. Должен также присутствовать механизм определения и контроля информации, передаваемой на домашнее рабочее место, получаемой с него, и используемой в процессе работы.

Необходимо наличие определенной политики по использованию оборудования для посторонней деятельности, такой, как компьютерные игры, доступ в Интернет, и т.п., так как любая такая деятельность может привести к проблемам при соседстве с важными и конфиденциальными данными.

6.8 Разработка и сопровождение информационных систем

6.8.1 Требования к безопасности систем

Цель: Обеспечить встраиваемость средств защиты в информационные системы.

Анализ и задание требований к безопасности

Бизнес-требования для новых систем или усовершенствования для существующих будут определять требования по средствам управления.

Руководство по аудиту:

Организации должны быть в состоянии продемонстрировать, что требования по безопасности были определены и приняты в расчет для разработки программ-приложений, новых систем, усовершенствования и модернизации систем. В реальности это представлено двумя категориями, где заданное ПО приложений разрабатывается конкретно для организации или самой организацией, или где уже готовое коммерческое ПО (COTS) приобретается для использования в защищенной среде. (Необходимо заметить, что ПО COTS может составлять целую программу-приложение или ее встраиваемый компонент.)

Начальный анализ требований необходим, чтобы идентифицировать вопросы безопасности и рассмотреть их в документах с пользовательскими требованиями к приложениям для новых систем и/или отчете об их оценке. По завершении данной процедуры аудитор должен посмотреть, как данные требования контролируются и проверяются во время разработки и внедрения системы. Любые проблемы должны быть проанализированы, подняты к рассмотрению на соответствующем уровне менеджмента и удовлетворительно решены.

6.8.2 Безопасность в прикладных системах

Цель: Предотвратить потерю, модификацию и несанкционированное использование пользовательских данных в прикладных системах.

6.8.2.1 Проверка достоверности входных данных и Проверка достоверности внутренней обработки данных

Ввод данных в системы-приложения будет подтвержден, чтобы удостовериться, что он произведен правильно и надлежащим образом.

Подтверждающие проверки будут включены в системы для определения любых сбоев в обработке данных.

Руководство по аудиту:

Программы приложения должны предоставлять надлежащий уровень проверки целостности данных, как во время ввода, так и во время обработки данных. Когда данные вводятся вручную, аудитор должен удостовериться, что очевидно неверные значения, не вписывающиеся в заданные рамки, неправильные значения и неполные данные не принимаются. В случае, если данные предоставляются в бумажной форме (для последующего ввода операторами), необходимо просмотреть, какое дается подтверждение для этих данных – могут ли данные документы быть оценены персоналом, не имеющим на это полномочий? В случае очевидных изменений, проверяются и утверждаются ли они? В случае ввода данных через другие каналы, такие как пленка или диск, необходимо удостовериться, что они маркированы

надлежащим образом и не искажается до использования. После того, как данные введены в систему, могут появляться ошибки из-за ошибок системы или нарочного изменения. В документации по разработке необходимо установить, какие еще проверки на целостность можно проводить и удостовериться, что они соответствуют требованиям и по возможности выполнять их. Разработка системы должна минимизировать риск того, что данные могут быть испорчены, а также гарантировать, что выполняются проверки для определения любой порчи данных.

6.8.2.2 Аутентификация сообщений

Для приложений с требования безопасности по защите целостности содержания сообщения будет использована аутентификация сообщений.

Руководство по аудиту:

Аудиторы должны спрашивать, применяется ли организацией аутентификация сообщений, и если да, то проверять, верно ли используются ее механизмы. Организация должна была провести оценку рисков для определения рисков и выяснить, нужна ли аутентификация сообщений для защиты целостности их содержимого, и если да, то какова наиболее подходящая форма ее внедрения. При проверке использованных методов, аудитор должен принимать в расчет результаты оценки рисков.

Примеры ситуаций, когда следует использовать аутентификацию сообщений, включают в себя:

– Обмен документами и сообщениями как часть некоей активности в области электронной торговли или другой электронной деятельности;

– Обмен электронными сообщениями и/или файлами;

– Любое другое приложение, где сохранность содержимого сообщения является важной или жизненно необходимой.

6.8.2.3 Проверка достоверности выходных данных

Выходные данные из системы-приложения должны быть проверены, чтобы удостоверить, что обработка хранимой информации является правильной и сообразной обстоятельствам.

Руководство по аудиту:

Система-приложение должна предоставлять четкие выходные данные и организация должна обладать механизмом проверки точности выходных данных и реакции на получение неверных или неполных выходных данных. Аудиторы должны принять участие в подобных проверках выходных данных, чтобы удостовериться, что персонал знаком с данными процедурами, искать возможные недоделки или возможности обойти данные процедуры. Они также должны проверять, чтобы ответственные за данные процедуры были определены и знали свои обязанности.

По окончании проверок тестов подтверждения выходных данных, необходимо удостовериться, что их результаты не могут быть изменены незаконным путем.

6.8.3 Криптографические средства контроля

Цель: Обеспечить защиту конфиденциальности, аутентичности или целостности информации.

6.8.3.1 Политика использования криптографических средств контроля

Необходимо разработать политику использования криптографических методов управления для защиты информации.

Руководство по аудиту:

Важным аспектом безопасного и эффективного использования криптографических элементов управления является удостоверение в том, что были приняты верные решения о механизмах использования и применяемой политике ежедневной поддержки данных элементов управления. Данная политика должна охватывать применяемый менеджментом ключевой подход, роли и обязанности, относящиеся к использованию криптографических элементов управления, информацию и обстоятельства в которых должны применяться криптографические элементы управления.

В случае, если организация применяет криптографические элементы управления, аудиторы должны удостовериться, что политика использования криптографических элементов управления была разработана, распространена, и все сотрудники знают ее и следуют ей. Они должны выяснять, поддерживаются ли принятые решения результатами оценки рисков, и соответствуют ли используемые элементы управления данной политике.

Сила криптографических элементов управления меняется и соотносится с используемыми алгоритмами и ключевыми размерами и параметрами. Необходимо учитывать среду и приложения, в которых используются криптографические элементы управления. Среды некоторых приложений могут требовать более сильных криптографических элементов управления.

Таким образом, аудиторам понадобятся по крайней мере общие знания криптографических техник и механизмов, ключевого менеджмента и их применения к ресурсам, чтобы сказать, подходят ли организации те методы, которые она использует.

6.8.3.2 Шифрование, Цифровые подписи и Сервисы обеспечения неотказуемости

Для защиты конфиденциальности уязвимой или критической информации должно применяться шифрование.

Для защиты аутентичности и целостности электронной информации должны применяться цифровые подписи.

Для решения спорных вопросов о наличии или отсутствии каких-либо событий или действий должны использоваться сервисы обеспечения неотказуемости.

Важным является то, что выбор и применение конкретных средств защиты информации, основанных на применении криптографических методов, регламентируется законодательством Республики Казахстан.

Руководство по аудиту:

Аудиторы также должны проверять условия, по которым применяется шифрование, цифровые подписи и/или сервисы обеспечения неотказуемости и соответствуют ли они законодательству Республики Казахстан и политике определенных бизнес-требований и требований безопасности.

Кроме того, они должны проверить, что:

– Использовалась оценка рисков при принятии решения об использовании или неиспользовании шифрования, цифровой подписи или сервисов обеспечения неотказуемости и определить точные требования по защите;

– Были выбраны подходящие алгоритмы и длина ключа и, что они сопоставимы с определенными требованиями по защите и результатами оценки рисков;

– Любое существующее законодательство, включая правила экспорта и импорта и процедуры, касающиеся использования приложений криптографических механизмов были определены и соблюдаются;

– Все надлежащие системы менеджмента ключей действуют в целях защиты ключей и гарантии их безопасного хранения и использования.

Аудиторы должны спрашивать и выяснять, знают ли служащие о политике криптографических элементов управления, и когда их следует использовать, например, наблюдая за использованием криптографического контроля.

6.8.3.3 Управление ключами

Для поддержки криптографических методов должна использоваться система управления ключами, основанная на согласованной совокупности стандартов, процедур и методов.

Руководство по аудиту:

Управление ключами является необходимым условием безопасного использования криптографических элементов управления; криптография не должна использоваться без готовой защищенной системы управления ключами. Аудиторы должны проверить, употребила ли организация необходимые элементы управления, чтобы защитить:

– секретные и частные ключи от раскрытия, изменения или разрушения;

– общественные ключи и сертификаты общественных ключей от несанкционированного изменения или разрушения; в случае, если организация пользуется услугами сертификационных руководителей (личных или общественных) для управления своими общественными ключами, необходимо удостовериться, что данные руководители адекватно защищены, надежны и управляемы.

Защита криптографических ключей должна совмещать и логическую, и физическую защиту. Аудиторы должны проверять физиологические и логические инструменты управления доступом, применяемые для защиты криптографических ключей. В случае, если механизм или процесс депонирования или восстановления ключа применяется к криптографическим ключам, необходимо удостовериться, что служащие об этом знают, и что не существует возможностей обойти депонирование ключа.

6.8.4 Безопасность системных файлов

Цель: Обеспечить надежную реализацию проектов разработки информационных систем и их поддержку

6.8.4.1 Контроль рабочего программного обеспечения

Должны существовать процедуры для контроля установки программного обеспечения в рабочих системах.

Руководство по аудиту:

Аудиторы должны проверить элементы управления, применяемые к внедрению ПО на ОС – как содержится системный код, включен ли источник кода, как вводятся новые версии, как защищаются системные файлы и библиотеки, какие записи делаются об изменениях? Разработчики и персонал поддержки должны быть в курсе возможных опасностей внедрения не протестированных или неразрешенных кодов в ОС, необходимо проверить, что они об этом осведомлены.

Затем необходимо обратить внимание на внедрение – какая защита применяется к кодам исходного текста и объекта, какие этапы тестирования должны быть завершены перед вводом нового или измененного ключа, правильно ли регрессивное тестирование, могут ли старые версии ключа быть проинсталлированы заново, сохраняется ли полная копия данных перед внесением изменений?

Необходимо просмотреть записи изменений в операционном коде, полные ли они, достаточно ли описательные и имеют ли надлежащее разрешение? Комплекс важнейших операций может потребовать тщательно продуманные детальные планы для ввода нового или измененного кода, просмотрите примеры.

6.8.4.2 Защита системных тестовых данных

Должна быть обеспечена защита и контроль тестовых данных.

Руководство по аудиту:

Аудиторы должны удостовериться, что данные, используемые для тестирования, контролируются надлежащим образом. Тесты должны быть воспроизводимыми и, таким образом, использованные данные должны быть четко выделены и доступны для повторного тестирования. Использование настоящих данных для тестирования не приветствуется и в случае

использования должна быть изменена, чтобы исключить любую личную или важную информацию. Это не всегда полностью возможно, или не всегда возможно это полностью гарантировать, поэтому необходимо проверить, каким образом защищены они или любые результаты тестов, включая и файлы, и записанные результаты.

Необходимо проверить, что использование настоящих данных для тестирования должно быть надлежащим образом санкционировано в каждом случае. Также необходимо проверить наличие готового метода для полного удаления любых данных, введенных в базу данных во время тестирования, и контроля доступа. Доступ к системам-приложениям по тестированию должен строго контролироваться, как и доступ к ОС.

6.8.4.3 Управление доступом к библиотекам исходных текстов программ

Должен осуществляться жесткий контроль доступа к библиотекам исходных текстов программ.

Руководство по аудиту:

Доступ к любым файлам с кодами источников должен быть защищен, лучше всего путем не хранения его в ОС. Доступ к такому коду и средствам пересортировки и перестановки ссылок может с легкостью обойти все дальнейшие проверки безопасности, обычно применяемые приложениями. Высоко-секретные приложения могут нуждаться в предоставлении подтверждения проверок суммы кода объекта для определения внесенных изменений.

Также необходимо рассмотреть программы отчетов макроса и базы данных, изменить которые может быть гораздо легче, и которые могут повлечь за собой потерю целостности или недоступность данных. Данные ограничения не должны регламентироваться только до возможных злоумышленных действий, обычные обновления и переустановка кода исходного текста приложений должна четко контролироваться с целью обеспечения записи и тестирования изменений перед тем, как будет разрешен доступ к настоящей и уязвимой информации. Аудиторы должны просмотреть задокументированные процедуры и записи.

6.8.5 Безопасность в среде разработки и рабочей среде

Цель: Обеспечить безопасность программного обеспечения прикладных систем и информации.

6.8.5.1 Процедуры управления процессом внесения изменений

Внесение изменений должно строго контролироваться с помощью формальных процедур управления процессом внесения изменений.

Руководство по аудиту:

Аудиторы должны проверить, что формальные процедуры контроля за изменениями применяются для всех изменений, вносимых в приложения в ОС и системной среде. Данные процедуры могут быть необходимы в планах по качеству больше, чем стандартные. Также необходимо проверить, что

такие же процедуры существуют и в поддержке и в случае необходимости обеспечивают изменения в создании и документах, касающихся требований.

В частности, необходимо проследить, как обращаются с изменениями онлайновых ОС (которые очень часто являются одними из важнейших), так как часто они требуют аккуратного и развернутого планирования. Предоставлены ли достаточные приготовления для поддержки при аварии? Доступ персонала поддержки к важным частям системы должен быть ограничен только к необходимому уровню, необходимо проверить, каким образом это выполняется. Нужно также проверить, все ли изменения санкционированы надлежащим образом (разрешение получено от верного уровня менеджмента и что операционный менеджмент вовлечен в процесс), что изменения правильно проверяются и тестируются, и что полное разрешение до того, как вводятся изменения.

Часто изменения группируются и встраиваются в версию, а не вводятся по заранее подготовленному плану, в данном случае необходимо проверить, что записи версий правильно определяют внесенные изменения. Вероятно, что процедура внесения срочных изменений также применяется, чтобы исправить ситуации отказа системы, необходимо проверить, чтобы это отвечало всем названным выше критериям. Проверьте, что соответствующий контроль конфигурации применяется во время изменений и, что правильные записи о внесенных изменениях сделаны.

6.8.5.2 Технический анализ изменений, вносимых в операционную систему

При внесении изменений в операционную систему должны проводиться анализ и тестирование прикладных систем.

Руководство по аудиту:

Организация должна обладать процедурой проверки изменений ОС. Она должна происходить перед плановым внедрением, по возможности тестовое внедрение должно быть оценено. Данная проверка должна включать в себя оценку элементов управления, которые должны быть готовы после изменений, и проверку того, что они соответствуют требованиям. Аудиторы должны просмотреть содержимое данных отчетов о проверках, такое как данные о производителях и примечания к версиям, данные об оценке в случае их наличия, определенные изменения ПО, которые понадобятся, например, в случае, если была использована обработка неисправностей ОС, и приготовлении поддержки.

Выводы из данных проверок должны включать в себя любые необходимые изменения приложений и план по внедрению новой версии ОС. Версия ОС (плюс любые программные коррекции) должна быть определена в конфигурационных записях. В некоторых случаях организации могут решить не обновлять систему, необходимо проверить, чтобы и в той ситуации у них

был доступ к необходимым уровням поддержки, и если его нет, это должно быть определено в оценке рисков и повлечь соответствующие действия.

6.8.5.3 Ограничения на внесение изменений в пакеты программ

Не рекомендуется модифицировать пакеты программ, все необходимые изменения должны строго контролироваться.

Руководство по аудиту:

Необходимо использовать надлежащим образом документированную и утвержденную процедуру контроля изменений. Любые изменения должны внедряться под контролем и с гарантией, что изменения полностью обоснованы и утверждены до внедрения. Программные пакеты должны изменяться только при условии существования деловых требований к этому.

Иногда изменения в коды могут вноситься в качестве программных коррекций, которые впоследствии будут встроены в следующие версии, в случае, если так происходит, необходимо удостовериться, что программная коррекция удалена и вся надлежащая документация обновлена. Иногда организации могут иметь доступ к программным источникам, однако они не обладают полномочиями разработчиков; права вносить изменения должны быть четко определены в контрактах, однако, необходимо удостовериться, что изменения внедряются надлежащим образом, так как из-за неимения полного доступа к записям разработчиков, могут быть привнесены дальнейшие риски для целостности системы. Также необходимо проверить, каким образом обращаются с подобными изменениями, когда устанавливаются новые версии оригинальной программы, так как они могут требовать переустановки. Необходимо проверить, что сохраняется полная история всех внесенных изменений, и что данные записи сохраняются столько, сколько требуется. Все программы-приложения должны иметь определенную последовательность регрессионных тестов, которые могут быть использованы для подтверждения работы измененного кода, необходимо просмотреть, как это контролируется.

6.8.5.4 Скрытые каналы и встроенный код типа «Троянский конь»

Закупка, использование и модификация программного обеспечения должны строго контролироваться и проверяться с целью защиты от возможных скрытых каналов и встроенного кода типа «Троянский конь».

Руководство по внедрению:

Почти все современные программные продукты содержат какой-либо вид скрытых каналов. Многие из них безвредны, например, как комбинации специальных ключей, передающих информацию о программистах, разрабатывавших ПО, однако некоторые могут быть опасны. Организации должны определить свое отношение к скрытым каналам, и решить, необходимо ли предпринять какие-либо действия по защите от них. Принимая такое решение, необходимо помнить, что скрытые каналы могут быть определены только в результате долгого и трудоемкого процесса. Код типа «Троянский конь» может быть встроен в систему незаметно, и может

использоваться для совершения нежелательных и незаметных для пользователя функций, таких как отсылка предварительно собранных кодов.

Руководство по аудиту:

Многие элементы ПО содержат различные формы скрытых кодов. Часть их, в общем, безвредны и не представляют угрозы. С другой стороны, некоторые из них могут быть использованы и могут стать путем для скрытых каналов, и их, как и «Троянского коня» не просто обнаружить.

Аудитор должен проверить, какие действия предусмотрены организацией для обращения со скрытыми кодами и кодом типа «Троянский конь» Необходимо принять во внимание, что скрытые каналы и код типа «Троянский конь» могут привести к несанкционированному разглашению, изменению или уничтожению информации.

6.8.5.5 Разработка программного обеспечения на условиях аутсорсинга

Должны применяться средства управления для защиты разработок программного обеспечения, выполняемых на условиях аутсорсинга.

Руководство по аудиту:

Организация должна исследовать риски по разработке программного обеспечения в условиях аутсорсинга. В идеале, среда разработки и входящие в нее процессы должны инспектироваться и проверяться. Риски, связанные с такой разработкой должны быть проверены, также в любом контракте на разработку необходимо охватить все требования безопасности, элементы управления и обязанности обеих сторон, относящихся к данной разработке, и любые выявленные риски. Аудиторы должны удостовериться, что подобный контракт охватывает следующие пункты:

– условия измерения временных рамок и качества разработанного ПО и требования к коду качества,

– права доступа в случае необходимости аудита для гарантии качества выполняемой работы,

– правила и соглашения, определяющие право на интеллектуальную собственность и принадлежность разрабатываемого ПО,

– тестирование достаточной функциональности разрабатываемого кода, включая проверки на вирусы, скрытые каналы и наличие кода типа «Троянский конь».

6.9 Планирование бесперебойной работы организации

6.9.1 Аспекты планирования бесперебойной работы организации

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

6.9.1.1 Процесс планирования бесперебойной работы организации и Бесперебойная работа организации и анализ влияния факторов

Должен существовать единый контролируемый процесс для разработки и реализации планов обеспечения бесперебойной работы для всей организации.

Для централизованного подхода к обеспечению бесперебойной работы организации должен быть разработан стратегический план, основанный на оценке соответствующих рисков.

Руководство по аудиту:

Планирование бесперебойной работы организации должно быть результатом процесса эффективной оценки рисков и достаточной защиты от прерывания бизнеса и аварий, которые должны проводиться в каждой организации. Сфера охвата и подробности данных планов должны соответствовать требованиям безопасности и ведения дел.

Аудиторы должны проверить, что процесс управления бесперебойной работой организации существует, поддерживается и применяется во всей организации.

Планирование бесперебойности работы организации должно быть основано на анализе рисков и последствий прерывания деловой активности. Аудиторы должны проверить, что оценка риска полная и охватывает все части организации, относящиеся к прерыванию деловой активности, а не сосредоточена только на службах обработки информации. Результаты оценки рисков и последствий должны использоваться для разработки плана обеспечения бесперебойной работы организации. Аудиторы должны удостовериться, что сфера охвата и подробности данного плана подчинены требованиям по безопасности и деловым требованиям данной организации, и подписаны менеджментом.

6.9.1.2 Составление и реализация планов обеспечения бесперебойной работы организации

Должны быть разработаны планы по обеспечению и своевременному восстановлению производственной деятельности в случае приостановки или отказов критических производственных процессов.

Руководство по аудиту:

Планы обеспечения бесперебойности работы организации должны быть сосредоточены на выполнении обозначенных требований бизнеса и безопасности, как описано выше. Аудиторы должны проверить, достаточны ли временные рамки, связанные с данными планами, удовлетворяют деловым требованиям и реалистичны ли они. Кроме того, необходимо проверить, что:

– все обязанности согласованы и закреплены;

– сотрудники в курсе своих обязанностей и что они должны делать в случае аварий или прерываний деловой активности;

– все процессы, определенные в планах, задокументированы и внедряются согласно расписанию;

– весь персонал в курсе и понимает, что они должны делать в случае аварий или прерываний деловой активности;

– планы тестируются и обновляются согласно определенному расписанию.

6.9.1.3 Единая система планов обеспечения бесперебойной работы организации

Должна существовать единая система планов обеспечения бесперебойной работы организации, обеспечивающая согласованность всех планов и определение приоритетов для тестирования и реализации.

Руководство по аудиту:

Во всех организациях, где существует несколько планов, касающихся нескольких отделов, или обслуживающих сценарии, необходимо удостовериться, что существует состоятельные рамки планов, необходимо проверить существование данных рамок и что планы не противоречат ей. Планы также не должны противоречить уровням обязательств по сервису, и это необходимо проверить.

Необходимо удостовериться, что план готов к использованию, что применяется надлежащий контроль над документами, и что ключевые сотрудники знают, что требуется изначально, и какие элементы являются обязательными – например, коды от сейфов, телефоны аварийных служб и т.д. – и знают их местонахождения. Необходимо просмотреть подбор персонала, полагается ли организация на одного или нескольких ключевых сотрудников, что произойдет, если они будут недоступны? Также следует просмотреть, требуется ли обновлять информацию, необходимую в экстренных случаях – имена и контактные телефоны, коды доступа и т.д. – необходимо проверить, что это выполняется.

Были ли рассмотрены такие типовые сценарии, как сбой данных, вирусная атака, пожар, потеря ключевого персонала, длительный перерыв в поставках? Существуют ли распоряжения по тестированию поддерживающих действий, восстановление данных, их передача или перенос и так далее?

6.9.1.4 Тестирование, реализация и обновление планов обеспечения бесперебойной работы организации

Планы обеспечения бесперебойной работы организации должны регулярно тестироваться и обновляться с целью обеспечения их эффективности.

Руководство по аудиту:

Тестирование планов обеспечения бесперебойной работы организации является обязательным, и аудиторы должны определить расписание тестирований, которое может быть определено в рамках плана, или в самом плане. Маловероятно, что планы с определенным уровнем сложности превосходно сработают с первого раза, люди должны следовать процедурам,

чтобы успешно справиться с данной ситуацией, и этого можно достичь только с практикой. Должен существовать определенный план разработки самих планов, полная проверка и обсуждение перед первым изданием, расписание тестов с последующим анализом и проверкой, наконец, проведение тестов без предупреждения для проверки их продолжительной пригодности и предоставления условий для тренировки сотрудников. Необходимо просмотреть результаты тестов, в которых были замечены какие-либо проблемы, были ли они проанализированы и исправлены, каковы были критерии оценки деятельности, соответствовали ли они должному уровню сервиса? Также необходимо просмотреть, были ли включены в тестирование новые сотрудники и третьи лица? Очень часто продолжение деятельности будет зависеть от эффективной кооперации. Обратите особое внимание на планы, которые не обновлялись регулярно, присутствуют ли записи о том, что их проверяли на действенность, охват новых возможностей, изменения в регулирующих требованиях? Необходимо проверить, что обязанности по поддержке и обновлению планов были определены, что любые изменения в планах могут вноситься только с соответствующего разрешения.

6.10 Соответствие формальным требованиям

6.10.1 Выполнение правовых требований

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

6.10.1.1 Определение необходимых требований

Все правовые и договорные требования, имеющие отношение к безопасности, должны быть определены в явном виде и задокументированы для каждой информационной системы.

Руководство по аудиту:

Организация должна показать аудиторам действия, предпринимаемые для определения и соответствия определенному законодательству. Аудиторы должны проверить, что ни одно применяемое законодательство не было забыто или ошибочно упущено. Организации должны обладать подготовленными элементами управления для соответствия ранее определенным законодательным правилам. Ответственность за данные элементы управления должны быть определены и задокументированы, а ответственные должны быть в курсе своих обязанностей.

6.10.1.2 Защита авторских прав

Должны быть реализованы необходимые процедуры по соблюдению правовых ограничений на использование материалов, защищенных законом об

авторском праве, и на использование патентованного программного обеспечения.

Руководство по аудиту:

Аудиторы должны просмотреть имеющиеся в организации процедуры защиты авторских прав на информацию и ПО. Данные процедуры должны описывать принципы обращения с материалом, помеченным как авторский, правами на разработку или торговыми марками, и служащие должны знать, как обращаться с подобными материалами. Пользователи также должны знать, что любое неразрешенное копирование или использование материалов или ПО, защищенных авторскими правами, могут привести к проблемам с законом.

Необходимы строгие элементы управления использованием ПО в организации. Аудиторы должны выяснить, какие лицензии были приобретены, и как поддерживается их соблюдение. Многие коммерческие пакеты предоставляют лицензионное соглашение на данный пакет, которое может иметь различные формы, не существует единого формата, поэтому для проверки такой информации, как число пользователей, ограничения по использованию, и проч., необходимо собрать дополнительные сведения для проверки соответствия действий лицензионному соглашению.

Одним из вариантов является рассмотреть, как организация обращалась с этим, возможно собрать набор ключевых пакетов и затем определить ключевые аспекты каждой лицензии, сравнив их с записями о настоящем использовании из инвентаризационных проверок. Необходимо просмотреть использование инструментов и библиотек разработки, правильно ли они использовались? В случаях с упомянутым выше ПО, разработанном для организаций, необходимо просмотреть контракт на разработку или поддержку, в случае, если предоставлен доступ к источникам, могут ли быть применены домашние изменения, существуют ли ограничения по использованию и местонахождению ПО. Необходимо удостовериться, что ответственные за это сотрудники организации полностью в курсе своих обязанностей относительно авторских прав на ПО. Проверьте несколько случайно выбранных персональных компьютеров на наличие нелицензированного ПО.

6.10.1.3 Защита документации организации

Важные для организации документы должны защищаться от потери, уничтожения и подделки

Руководство по аудиту:

Записи, необходимые для законных или регулирующих целей, как правило, представляют собой часть всех записей, которые потребуются организации для ведения бизнеса или в каких-либо других целях. Необходимо удостовериться, что все необходимые для законных или регулирующих целей определены и соответствуют всем требованиям. Сюда

могут входить, например, финансовые отчеты, таможенные записи, правовые записи и записи касательно окружающей среды. Точные требования могут меняться в зависимости от страны, и организация должна быть в курсе и соблюдать соответствующие требования. Необходимо удостовериться, что это выполняется и заверено соответствующим персоналом. Распоряжения по хранению (включая распоряжения относительно безопасности), требования по проверке и владению должны быть определены в процедурах.

Должна существовать некая форма четко определенного списка, какие записи туда включены, и аудиторы должны проверить его точность. Некоторая информация может храниться в электронном виде, в оригинальном или отсканированном формате. Необходимо проверить, проверила ли организация законность этого метода хранения и соответствует ли он конкретным требованиям.

6.10.1.4 Защита данных и конфиденциальность персональной информации

Должны применяться средства контроля для защиты персональной информации в соответствии с действующими правовыми нормами.

Руководство по аудиту:

В Великобритании для соблюдения Акта о Защите Данных необходим четкий контроль личной информации; во многих других странах, например, в Европе, существуют аналогичные законы. Законодательство также может требовать от организации регистрации того, что она использует, и это необходимо проверить. Также необходимо проверить тип используемых данных, необходимо, чтоб они были подтверждены, передаются ли они за пределы организации? Кто имеет доступ к этим данным, необходимо ли это для их работы?

Необходимо проверить, контролирует ли организация изменения в требованиях в данной области, новые, более жесткие ограничения могут быть введены с указанным сроком для выполнения. Знают ли об этом, существуют ли планы внедрения изменений в указанные временные рамки? Аудиторы должны гарантировать, что они сами полностью осведомлены о данных аспектах законодательства.

6.10.1.5 Предотвращение незаконного использования информационных ресурсов

Использование информационных ресурсов должно санкционироваться руководством. Для защиты от незаконного использования этих ресурсов должны применяться соответствующие средства управления.

Руководство по аудиту:

Злоупотребление средствами обработки информации может повлечь за собой не только повышенные траты организации на оплату телефонных переговоров, дополнительной траты дискового пространства, времени процессора, загрузки сети, потере рабочего времени и т.д., но и может привести к непреднамеренному разглашению, порче важной информации или

доступу к ней из неразрешенных источников. Это также может повлечь за собой злоумышленное заражение ПО, такое как запуск вирусов, «Троянских коней» и т.д. или к нарушению законодательства, в случае, если средства обработки информации, принадлежащие данной организации, используются сотрудниками, совершающими противоправные действия.

Должна существовать четкая политика, определенная менеджментом и понятая и формально признанная работниками. В случае, если сотрудникам разрешается использовать компьютеры для игр, доступа в Интернет и т.п., то они должны быть отделены от тех, которые работают с важной информацией. Необходимо исследовать использование другого, удаленного оборудования, такого как принтеры, копиры и т.д. – какова политика в их отношении?

6.10.1.6 Регламентирование использования криптографических средств контроля

Должны существовать средства управления, обеспечивающие выполнение требований национальных соглашений, законов, инструкций или других документов по регламентированию доступа к криптографическим средствам контроля или использования этих средств.

Руководство по аудиту:

Организация должна продемонстрировать аудиторам действия, которые были предприняты для выявления соответствующего законодательства и правил для криптографических элементов управления, а также прибегали ли они в случае необходимости к юридической консультации, для соблюдения законодательства. Элементы управления, используемые для выполнения данных требований, должны быть задокументированы, внедрены и получена надлежащая поддержка. Аудитор должен проверить, чтобы внедрение криптографических элементов управления, как описано в разделе 2.8.3, соответствуют определенным правовым требованиям.

6.10.1.7 Сбор доказательств

В случае если действия, направленные против личности или организации, требуют разбирательства в соответствии с законодательством (гражданским или уголовным), предоставляемые доказательства должны удовлетворять правилам, сформулированным в соответствующих законах, или правилам конкретного суда, в котором будет рассматриваться этот случай. Кроме того, должны выполняться требования всех опубликованных стандартов или общепринятых правил по получению разрешенных доказательств.

Руководство по аудиту:

Сбор доказательств важен, чтобы иметь возможность предоставить адекватную поддержку для правовых процедур и действий, которые могут последовать как результат нарушения гражданского или уголовного права. Организация должна обладать подготовленными процедурами для сбора

свидетельств, и аудиторы должны проверить, что данная процедура гарантирует, что:

– собранная информация соответствует применяемым стандартам или практикам для предоставления подобных свидетельств в качестве улик;

– качество и полнота данных улик (то есть их весомость) достаточны;

– полнота и правильность информации может быть доказана.

Аудиторы должны проверить, где хранятся собранные свидетельства, и возможно ли несанкционированно изменить или уничтожить данные свидетельства. Кроме того, аудиторы должны рассмотреть условия, когда необходимо начать сбор улик. Их сбор должен начаться на ранней стадии, чтобы гарантировать, что информация не уничтожается.

6.10.2 Проверка безопасности информационных систем

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

6.10.2.1 Соответствие политике безопасности

Управляющий персонал организации должен принимать меры по обеспечению надлежащего выполнения процедур безопасности, находящихся в их зоне ответственности. Все подразделения организации должны регулярно проверяться с целью обеспечения соответствия принятой политике и стандартам безопасности.

Руководство по аудиту:

Для определения степени выполнения политики процедур по обеспечению безопасности, менеджмент должен гарантировать проведение внутреннего аудита. Они должны быть запланированы и выполняться компетентными сотрудниками, полностью документироваться и отслеживаться для гарантии устранения несоблюдения, а также о них должны отчитываться руковод-тву. Периодичность проверок должна зависеть от требований безопасности, и аудиторы должны рассматривать вопрос о том, соответствует ли данная частота уровню риска, важности информации, изменениям в технологии и любым другим факторам, которые могут повлиять на организацию.

6.10.2.2 Техническая проверка на соответствие стандартам безопасности

Информационные ресурсы должны регулярно проверяться на соответствие стандартам обеспечения безопасности.

Руководство по аудиту:

Организации должны проверять, соответствуют ли их системы стандартам безопасности и внедрения. Должен существовать план проверки соответствия, отражающий, что должно проверяться, с какой частотой и какими методами. Необходимо, чтобы такой тип проверок на соответствие проводился достаточно квалифицированным для этого персоналом, или, по крайней мере, под его контролем. В случае использования инструментов, необходимо оценить, какие аспекты средств они действительно покрывают,

это может быть исключительно мониторинг или аудит средств – были ли они каким-либо образом утверждены? Необходимо проверить сотрудников, выполняющих и проверяющих проверки; зачастую полностью оценить соответствие сможет только технически компетентный персонал.

6.10.3 Аудит систем

Цель: Максимизировать эффективность и минимизировать воздействие на процесс аудита системы и со стороны процесса аудита.

6.10.3.1 Средства аудита систем

Для минимизации риска возникновения сбоев в производственных процессах аудит рабочих систем должен тщательно планироваться и согласовываться.

Руководство по аудиту:

Использование элементов управления и инструментов аудита системы не должно приводить к сбоям в информации и проверяемых системах. В случае, если проверки запланированные, необходимо удостовериться, что было получено необходимое разрешение от операционного менеджмента. Информация не должна изменяться ради цели данных действий и доступ к информации должен быть записан, как и для любой другой операции. Также необходимо гарантировать, что прерывания деловой активности сведены к минимуму. Необходимо удостовериться, что результаты аудита сохраняются, а использование любых инструментов записывается надлежащим образом. Также следует проверить, что сами инструменты формально утверждены перед использованием.

6.10.3.2 Защита средств аудита систем

Доступ к средствам аудита систем должен защищаться с целью предотвращения любых возможностей неправомерного использования или компрометации.

Руководство по аудиту:

Данные инструменты разрешат доступ к информации и элементам управления, которые можно было бы использовать для чтения или изменения важной информации. В чужих некомпетентных руках данные инструменты могут быть очень опасны, и необходимо осуществлять строгий контроль за тем, как они применяются.

По возможности, данные инструменты должны храниться отдельно от операционных и тестирующих систем; в случае, если инструменты хранятся в системе постоянно, каковы инструменты управления доступом?

Приложение
(справочное)
Библиография

[1] БИС РД 3003:2002 «Готовы ли вы к аудиту на соответствие стандарту BS 7799-2» («Are you ready for a BS 7799-2 audit»);

[2] БИС РД 3004:2002 «Руководство по реализации и аудиту средств управления стандарта BS 7799» («Guide to the implementation and auditing of BS 7799 controls»).

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