ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ ЖҮЙЕЛЕРІ
Талаптар

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
Требования

ҚР СТ ИСО/МЭК 27001-2008

(ИСО/МЭК 27001:2005 «Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар», IDT)

Ресми басылым

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

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ ЖҮЙЕЛЕРІ

Талаптар

ҚР СТ ИСО/МЭК 27001-2008

(ИСО/МЭК 27001:2005 «Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар», IDT)

Ресми басылым

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

Астана

Алғысөз

1 «Инфосистемы Джет» ЖАҚ **ӘЗІРЛЕДІ**

Қазақстан Республикасының Ақпараттандыру және байланыс агенттігі **ЕНГІЗДІ**.

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

3 Осы стандарт Қазақстан Республикасының экономикасының қажеттігін көрсететін қосымша талаптар мәтін бойынша көлбеу қаріппен белгіленіп ИСО/МЭК 27001:2005 «Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар» («Information technology. Security techniques. Information security management systems. Requirements), IDT, халықаралық стандартына балама.

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

Кіріспе

Осы стандарт ақпараттық қауіпсіздікті басқару жүйесін (АҚБЖ) әзірлеу, іске асыру, пайдалану, мониторинг, талдау, алып жүру және жаңарту үшін үлгілер ретінде пайдалану үшін дайындалған. АҚБЖ қабылдау ұйым үшін стратегиялық шешім болып табылуға тиіс. Ұйымдардың АҚБЖ архитектурасы мен іске асыруға бизнестің мақсаттары және қажеттіліктері, қауіпсіздікке қойылатын талаптар, пайдаланылатын рәсімдер, сондай-ақ ұйымның өзінің мөлшері мен құрылымы да әсер етеді. Уақыт өте келе аталған сипаттамалар және оларды қолдайтын жүйелер өзгереді деп болжанады. АҚБЖ іске асыру ұйымның қажеттіліктеріне сәйкес ауқымданады деп болжанады.

Осы стандарт мүдделі ішкі және сыртқы тараптардың сәйкестікті бағалау үшін пайдаланылуы мүмкін.

Осы стандартта ұйымдардың АҚБЖ әзірлеуге, іске асыруға, пайдалануға, қадағалауға, талдауға, ілестіруге және жетілдіруге процестік тәсіл қабылданған.

Тиімді қызмет істеу үшін ұйым әр түрлі әрекеттерді басқаруға және сәйкестендіруге тиіс. Кіріс деректерін шығыс деректеріне түрлендіру мақсатында басқарылатын және ресурстарды пайдаланатын кез келген әрекет процесс ретінде қарастырылуы мүмкін. Бір процесстің шығыс деректері келесі процесс үшін тікелей кіріс деректерін білдіреді.

Осы процесстерді сәйкестендіру және өзара әрекет етумен, сондай-ақ осы процесстерді басқарумен бірге ұйымда процесстер жүйесін қолдану «процестік тәсіл» деп аталуы мүмкін.

Осы стандартта берілген ақпараттық қауіпсіздікті басқаруға процестік тәсіл мыналарға ерекше мән беруге өздерінің пайдаланушыларын ниеттендіреді:

a) ұйымның ақпараттық қауіпсіздік талаптарын түсінуге және ақпараттық қауіпсіздіктің саясаты мен мақсаттарын айқындау қажеттігіне;

b) ұйымның ортақ бизнес-тәуекелдігінің мағыналы мәтініндегі ұйымның ақпараттық қауіпсіздігінің тәуекелін басқару үшін басқару қаражаттарын енгізуге және пайдалануға;

c) АҚБЖ өнімділігі және тиімділігінің мониторингі және талдауына;

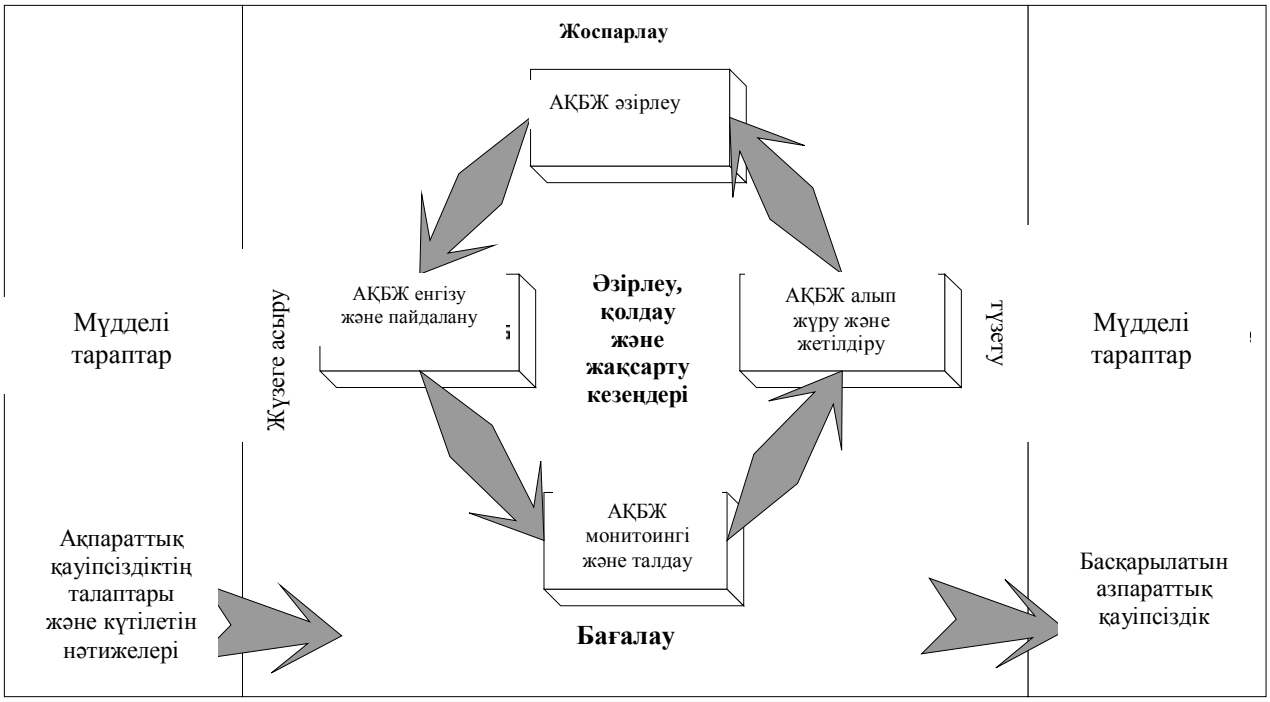
d) нақты көрсеткіштерге негізделген үздіксіз жетілдіруге.

Осы стандартта АҚБЖ барлық процесстерін құрылымдау үшін қолданылған «Жоспарлау – Іске асыру – Бағалау – Түзету - ПРОК» («Plan-Do-Check-Act» – PDCA) үлгісі қабылданған.

1-суретте ақпараттық қауіпсіздікке талаптарды және мүдделі тараптардың үмітін АҚБЖ кіріс деректері ретінде қалай қабылдайтыны көрсетілген және бірқатар қажетті әрекеттер және процесстер нәтижесінде

осы талаптар мен үміттерді қанағаттандыратын ақпараттық қауіпсіздіктің шығысын береді. Одан басқа,

1-суретте **4**, **5**, **6, 7** және **8**-тармақтарда берілген процесстердегі байланыстар көрсетілген.



1-сурет – АҚБЖ процесстеріне ПРОК үлгісін қолдану

ПРОК үлгілерін қабылдау сонымен бірге ақпараттық жүйелер және желілердің қауіпсіздігі жөніндегі нұсқамалық құжатта, OECD Guidelines (2002)[1], құжатта мазмұндалған қағидаларды да көрсетеді. Осы стандарт аталған құжатта мазмұндалған қауіпсіздіктің тәуекелдер бағасын, жоспарлауды және іске асыруды реттейтін, қауіпсіздікті және қайта бағалауды басқаратын қағидаларды іске асыру үшін тұрақты үлгіні ұсынады.

1-Мысал - Мыналар талаптардың бірі болуы мүмкін: ақпараттық қауіпсіздіктің зияндары ұйымға елеулі қаржылық залал келтірмеуге тиіс және/немесе ұйымның қызметіне қиындықтар туғызбауға тиіс.

2-Мысал - Мыналар үміттердің бірі болуы мүмкін: елеулі оқыс оқиға болған жағдайда (мысалы, электрондық бизнес үшін пайдаланылатын ұйымның web-сайтына сәтті шабуыл жасалғанда) қызметкерлердің әрекетті азайту үшін тиісті рәсімдерді пайдалануға жеткілікті дайындығы болады.

Жоспарлау (АҚБЖ әзірлеу)	Ұйымның жалпы саясаттарына және мақсаттарына сәйкес келетін нәтижелер алу мақсатында ақпараттық қауіпсіздікті арттыру және тәуекелдікті басқару үшін мәнді АҚБЖ

[1] OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

	саясатын, мақсаттарын, процесстерін және рәсімдерін айқындау.
Іске асыру (АҚБЖ енгізу және пайдалану)	АҚБЖ саясатын іске асыру және пайдалану, басқару, процесстер және рәсімдер құралдары.
Тексеру (АҚБЖ мониторингі және талдау)	Бағалау және егер талап етілсе, АҚБЖ саясатына, мақсаттарына және практикалық тәжірибеге сәйкестігін тексеру үшін процесс сипаттамасын өлшеу, сондай-ақ басқарушы қызметкерлермен әрі қарай талдау үшін нәтижелерді табыстау.
Жетілдіру (АҚБЖ алып жүру және жетілдіру)	АҚБЖ үздіксіз жетілдіру мақсатында АҚБЖ ішкі аудит және басқарушы қызметкерлермен орындалған талдау нәтижелері бойынша, сондай-ақ басқа мәні бар ақпараттың негізінде түзету және ескерту шараларын қабылдау.

Осы стандарт басқарудың жақын стандарттарымен біріктірілген және үйлесімді, орындалуды және қолдануды қамтамасыз ету үшін *ҚР СТ 9001:2001* және ISO 14001:2004 стандарттарымен келісілген. Осы үлгімен, осылай бір тиісті жолмен әзірленген басқару барлық осы стандарттардың талаптарын қанағаттандыра алады. В.1-кестесі (В қосымша) осы стандарттың, *ҚР СТ ИСО 9001:2001* стандарты *Сапа менеджменті жүйесі. Талаптар* және халықаралық ISO 14001:2004 стандарты (*Қолданыстағы стандарт ҚР СТ ИСО 14001-2000 Қоршаған ортаны басқару жүйелері. Қолдану жөніндегі талаптар және нұсқаулар)* тармақтары арасындағы өзара байланысты көрсетеді.

Осы стандарт ұйымның көрсетілген басқару жүйелеріне талаптарға сәйкес өзінің АҚБЖ біріктіре немесе тұрғыза алатындай етіп әзірленген.

МАҢЫЗДЫ! Осы стандарт ақпараттық қауіпсіздікті қамтамасыз ету үшін оған барлық қажеттілер енгізілген деп түсіндірмейді. Пайдаланушылар стандартты дұрыс қолдану үшін жауапкершілік көтереді. Стандартқа сәйкестік өзінен өзі құқықтық міндеттемелерден босатпайды.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ
АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ ЖҮЙЕЛЕРІ
Талаптар

Енгізілген күні 2008.07.01

1 Қолданылу саласы

Осы стандарт барлық тұрпаттағы ұйымдар үшін (мысалы, коммерциялық кәсіпорындарға, үкіметтік мекемелерге, коммерциялық емес ұйымдарға) қолданылады. Осы стандарт ұйымның ортақ бизнес тәуекелінің мағыналы мәтінінде құжаттандырылған **ақпараттық қауіпсіздікті басқару жүйесін** (бұдан әрі – АҚБЖ) әзірлеуге, іске асыруға, пайдалануға, мониторингке, талдауға, алып жүруге және жетілдіруге талаптарды айқындайды. Ол жеке ұйымдар немесе олардың бөлімдерінің тиісті қажеттіктеріне, басқару құралдарына талаптарды айқындайды.

АҚБЖ мүдделі тараптар үшін құпиялықты қамтамасыз ететін және ақпараттық ресурстарды қорғайтын бара бар және мөлшерлес қауіпсіздікті қорғау құралдарын қамтамасыз ету үшін әзірленеді.

Ескертпе 1 – Осы стандартта «бизнес» терминін кең мағынада түсіну керек, осы терминмен ұйым әрекетін жалғастыратын мақсаттарға жету үшін қажет кез келген қызмет көрсетіледі.

Ескертпе 2 – ISO/IEC 17799 стандартында басқару құралдарын әзірлеу кезінде пайдалануға болатын қолдану жөніндегі нұсқау келтіріледі.

Осы стандартта айқындалған талаптар ортақ болып табылады және олардың тұрпатына, мөлшеріне және қызмет түрлеріне тәуелсіз барлық ұйымдардың пайдалануы үшін арналған. Егер ұйым осы стандартқа сәйкестік туралы жарияласа, 4, 5, 6, 7 және 8 тармақтарда келтірілген талаптардың кез келгенін шығаруға жол берілмейді.

Тәуекелдерді қабылдау критерийлеріне сәйкестік үшін қажетті деп танылған басқару құралдарының барлық шығарылулары негізделуге тиіс және тәуекелдерді қабылдау туралы тиісті шешімдерді жауапты тұлғалармен қабылданғанына дәлелдеме берілуге тиіс. Егер қандай да бір басқару құралы шығарылатын болса, шығару тәуекелдерді бағалау нәтижелері бойынша және заң және нормативтік құжаттардың тиісті талаптарымен айқындалатын қауіпсіздікке талаптарды қанағаттандыратын ұйымның ақпараттық қауіпсіздікпен қамтамасыз ету міндеттемесіне және/немесе қабілеттілігіне әсер етпейтін жағдайлардан басқа, осы стандартқа сәйкестік туралы мәлімдемеге рұқсат етілмейді.

Ресми басылым

Ескертпе – Егер ұйымның бизнес-процестерді басқарудың қолданыстағы жүйесі болса (мысалы, *ҚР СТ ИСО 9001* немесе СТ РК ИСО 14001 стандартына сәйкес келетін), онда көпшілік жағдайда осы қолданыстағы басқару жүйесі шеңберінде осы стандарттың талаптарын қанағаттандырған дұрыс.

2 Нормативтік сілтемелер

Мына нормативтік-анықтамалық құжаттар осы стандартқа қолдану үшін міндетті. Егер құжаттың күні көрсетілсе, онда тек құжаттың көрсетілген редакциясын ғана пайдалану керек. Егер құжаттың күні көрсетілмесе, көрсетілген құжаттың (барлық түзетулер кіретін) соңғы редакциясы пайдаланылады.

ISO/IEC 17799:2005, Information technology — Security techniques - Code of practice for information security management [ISO/IEC 17799:2005, Ақпараттық технологиялар – Қауіпсіздік әдістері – Ақпараттық қауіпсіздікті басқару жөніндегі практикалық нұсқау]

3 Терминдер мен анықтамалар

Осы стандартта сәйкес анықтамаларымен мынадай терминдер қолданылады:

3.1 Тәуекелді талдау (risk analysis): Тәуекелдің туындау және бағалау көздерін сәйкестендіру үшін ақпаратты жүйелі түрде пайдалану. [ISO/IEC Guide 73:2002]

3.2 Қол жетушілік (availability): Авторластырылған пайдаланушының (мәнділік) талап етуі бойынша пайдалануға дайын және қол жетерлік болу қасиеті [ISO/IEC 13335-1:2004]

3.3 Ақпараттық қауіпсіздік (information security): Ақпараттың құпиялығын, тұтастығын және қол жетімділігін қамтамасыз ету; одан басқа, шынайылық (authenticity), есеп берушілік (accountability), бас тартпаушылық (non-repudiation) және сенімділік (reliability) сияқты басқа қасиеттер де тартылуы мүмкін. [ISO/IEC 17799:2005]

3.4 Ақпараттық қауіпсіздіктің оқыс оқиғасы (information security incident): Ақпараттық қауіпсіздікке қауіп-қатер және бизнес-ақпараттың беделін түсіру ықтималдығы зор болатын ақпараттық қауіпсіздіктің бірлі-жарым оқиғалары немесе бірқатар орынсыз және кездейсоқ оқиғалары. [ISO/IEC TR 18044:2004]

3.5 Құпиялық (confidentiality): Ақпараттың авторластырылмаған пайдаланушы, мәнділік немесе процесстер үшін ашылмайтын және қол жетпейтіндей болу қасиеті. [ISO/IEC 13335-1:2004]

3.6 Тәуекелді өңдеу (risk treatment): Тәуекелді өзгерту үшін шаралар таңдау және қолдану процессі. [ISO/IEC Guide 73:2002]

Ескертпе – Осы стандартта «басқару құралы» (control) термині «шара» (measure) терминінің синонимі ретінде пайдаланылады.

3.7 Тәуекелдің деңгейін айқындау (risk evaluation): Тәуекелдің мәнділігін айқындау үшін берілген критерийлермен бірге бағаланған тәуекелді салыстыру процессі. [ISO/IEC Guide 73:2002]

3.8 Қалдық тәуекел (residual risk): Тәуекелді өңдегеннен кейін қалған тәуекел. [ISO/IEC Guide 73:2002]

3.9 Тәуекелді бағалау (risk assessment): Өзіне тәуекелді талдау және тәуекелдер деңгейін айқындау кіретін толық процесс. [ISO/IEC Guide 73:2002]

3.10 Қолданушылық туралы ереже (statement of applicability): Ұйымның АҚБЖ-не қолданылатын және мәнді деп танылған басқару құралдары және басқару мақсатын сипаттайтын құжат.

Ескертпе – Басқару мақсаты және басқару құралдары ақпараттық қауіпсіздікке ұйымның тәуекелді бағалау және тәуекелдерді өңдеу процесстерінен, құқықтық және нормативтік талаптардан, шарттық міндеттемелерден және бизнес-талаптардан алынған нәтижелер және қорытындыларға негізделеді.

3.11 Тәуекелді қабылдау (risk acceptance): Тәуекелді қабылдау бойынша шешім. [ISO/IEC Guide 73:2002]

3.12 Ресурс (asset): Ұйым үшін құндылығы бар кез келген мән. [ISO/IEC 13335-1:2004].

3.13 АҚБЖ, ақпараттық қауіпсіздікті басқару жүйесі (information security management system, ISMS): Ақпараттық қауіпсіздікті әзірлеу, іске асыру, пайдалану, мониторинг, талдау, алып жүру және жетілдіру үшін арналған және бизнес-тәуекелдігін бағалауға негізделген басқару жүйесінің жалпы бөлігі.

Ескертпе – Басқару жүйесінің өзіне ұйымдастыру құрылымы, саясаты, жоспарларды әзірлеу, жауапкершіліктерді үлестіру, нұсқаулар, рәсімдер, процесстер және ресурстар кіреді.

3.14 Ақпараттық қауіпсіздік оқиғасы (information security event): Ақпараттық қауіпсіздік саясатының ықтимал бұзылуын немесе қорғаныс құралдарынан бас тартуды (safeguards), не болмаса қауіпсіздік үшін елеулі болуы мүмкін бұрын белгісіз жағдайды көрсететін жүйелер немесе желілер жағдайын сәйкестендіру жағдайы. [ISO/IEC TR 18044:2004]

3.15 Тәуекелді басқару (risk management): Бар тәуекелді ескере отырып ұйымды басқару және жетекшілік етуге бағытталған үйлестірілген әрекеттер. [ISO/IEC Guide 73:2002]

3.16 Тұтастық (integrity): Ресурстардың нақтылығын және толықтығын сақтау қасиеті. [ISO/IEC 13335-1:2004].

4 Ақпараттық қауіпсіздікті басқару жүйесі

4.1 Жалпы талаптар

Ұйым өзі кездесетін тәуекелдер және ұйымның жалпы бизнес-қызметінің мағыналы мәтініндегі құжаттандырылған АҚБЖ әзірлеуге, іске

асыруға, пайдалануға, мониторинг және талдау жүргізуге, алып жүруді және жетілдіруді жүзеге асыруға тиіс. Осы стандарттың мақсаттары үшін пайдаланылатын процесс 1-суретте берілген ПРОК үлгісіне негізделеді.

4.2 АҚБЖ әзірлеу және басқару

4.2.1 АҚБЖ әзірлеу

Ұйым мыналарды орындауға тиіс:

а) Бизнестің, ұйымның, оның орналасқан жерінің, ресурстары және технологияларының сипаттамаларының терминдеріндегі АҚБЖ шекарасын және қолдану салаларын айқындауға тиіс, бұл жағдайда қолдану саласынан барлық шығарылымдар үшін толық негіздеме келтірілуге тиіс (1.2 қараңыз).

б) Бизнестің, ұйымның, оның орналасқан жерінің, ресурстары және технологияларының сипаттамаларының терминдеріндегі АҚБЖ саясатын айқындау; бұл саясат:

1) өзіне мақсаттарды айқындау үшін жалпы құрылымды енгізеді, сондай-ақ ақпараттық қауіпсіздікті ескере отырып, қызметтің қағидаларын және басқарудың жалпы міндеттерін айқындайды;

2) өндірістік және құқықтық немесе нормативтік талаптарды, сондай-ақ шарттық міндеттемелерді ескереді;

3) АҚБЖ алып жүру және әзірлеу жүзеге асырылатын ұйымның стратегиялық тәуекелді басқарудың мағыналы мәтінін ескереді;

4) тәуекел деңгейі айқындалатын критерийлерді белгілейді (**4.2.1**с) қараңыз);

5) басшылықпен бекітіледі.

Ескертпе – Осы стандарттың мақсаттары үшін АҚБЖ саясаты ақпараттық қауіпсіздіктің көптеген (кең түрдегі көптеген) саясаты ретінде қарастырылады. Осы саясаттар бір құжатта сипатталуы мүмкін.

в) Тәуекелді бағалауға ұйымның тәсілін айқындайды.

1) Нақты АҚБЖ сәйкес келетін, бизнес-ақпараттың қауіпсіздігі талаптарына, сондай-ақ құқықтық және нормативтік талаптарға сәйкестендірілген тәуекелді бағалау әдістерін сәйкестендіреді.

2) Тәуекелді қабылдау үшін критерийлерді әзірлеу және тәуекелдің құптауға лайық деңгейін сәйкестендіреді (5.1е) қараңыз).

Тәуекелді бағалаудың таңдалған әдісі тәуекелді бағалау рәсімдерінің жаңғыртылған және салыстырмалы нәтижелеріне кепілдік беруге тиіс.

Ескертпе – Тәуекелді бағалаудың әр түрлі әдістері бар. Тәуекелді бағалаудың әдістерінің мысалдары ISO/IEC TR 13335-3 стандартында, Information technology— Guidelines for the management of IT Security — Techniques for the management of IT Security (ISO/IEC TR 13335-3, Ақпараттық технологиялар — АТ қауіпсіздігін басқару қағидалары — АТ қауіпсіздігін басқару әдістері) талқыланады.

г) Тәуекелдерді сәйкестендіру.

1) АҚБЖ қолдану саласына қатысты ресурстарды және осы ресурстардың иегерлерін1 сәйкестендіру.

2) Осы ресурстарға қатерлерді сәйкестендіру.

3) Осы қатерлерді іске асыру үшін пайдаланылуы мүмкін осалдықты сәйкестендіру.

4) Құпиялықты, тұтастықты және қол жетерлікті бұзу ресурстарына әсер етуі мүмкін әрекетті сәйкестендіру.

д) Тәуекелдерді талдау және бағалау.

1) Ресурстардың құпиялығын, тұтастығын немесе қол жетімділігін бұзу салдарын назарға ала отырып, қауіпсіздікті бұзуы мүмкін бизнеске әрекет етуді ұйым ауқымында бағалау.

2) Осы ресурстарға байланысты қауіп-қатерлер, осалдықтар және әсер етулердің басым болуындағы қауіпсіздікті бұзуды іске асырудың нақты ықтималдығын, сондай-ақ осы сәтте іске асырылған басқару құралдарын бағалау.

3) Тәуекелдер деңгейін бағалау.

4) 4.2.1в) 2) айқындалған тәуекелдерді қабылдау критерийлерін пайдалана отырып, тәуекелдер құптауға лайық болып табылады ма немесе өңдеуді талап ете ме, соны айқындау.

е) Тәуекелдерді өңдеу нұсқаларын сәйкестендіру және бағалау.

Мүмкін әрекеттерге мыналар жатады:

1) басқарудың тиісті құралдарын пайдалану;

2) олар ұйымның саясатын және тәуекелдерді қабылдау критерийлерін нақты қанағаттандырған жағдайда тәуекелдерді саналы түрде және әдейі қабылдау (4.2.1в) 2) қараңыз);

3) тәуекелдерді болдырмау;

4) байланыстырылған бизнес-тәуекелдерді басқа тараптарға, мысалы, сақтандырушыларға және жеткізушілерге табыстау.

ж) тәуекелдерді өңдеу үшін басқару мақсаттары және басқару құралдарын таңдау.

Басқару мақсаттары және басқару құралдары тәуекелдерді бағалау және тәуекелдерді өңдеу процесстерімен сәйкестендірілген талаптарды қанағаттандыратындай таңдалынып алынуға және іске асырылуға тиіс. Бұл таңдау жағдайында тәуекелдерді қабылдау критерийлері (4.2.1в)2) қараңыз), сондай-ақ құқықтық және нормативтік талаптар, шарттық міндеттемелер де ескерілуге тиіс.

---

[1] «Иегер» (owner) термині ресурстардың тиімділігін, әзірленімін, алып жүру, пайдалану және қауіпсіздігін бақылау (controlling) үшін тиісті жолмен бекітілген әкімшілік жауапкершілік жүктелген тұлғаны немесе мәнді білдіреді. «Иегер» термині осы ресурсқа осы тұлғаның қандай да бір меншік құқығы бар дегенді білдірмейді.

Осы процесстің бір бөлігі А қосымшасынан басқару құралдарын және басқару мақсаттарын таңдау болуға тиіс, таңдау нәтижесінде барлық сәйкестендірілген талаптар қанағаттандырылуға тиіс.

А қосымшасында келтірілген басқару мақсаттары және басқару құралдарының тізімі жеткілікті болып табылмайды, сонымен бірге қосымша басқару мақсаттары және басқару құралдары таңдап алынуы мүмкін.

Ескертпе – А қосымшасында ұйымда мәнді болып табылатын басқару мақсаттары және басқару құралдарының толық тізімі мазмұндалады. Осы стандартты пайдаланушыларға басқарудың бірде бір маңызды нұсқалары анықталмай қалмауға кепілдік беретін басқару мақсаттары және басқару құралдарын таңдау үшін басталған нүкте ретінде А қосымшасына бағдарлану ұсынылады.

з) Ұсынылатын қалған тәуекелдерді бекітуге басшылардан рұқсат алуға.

и) АҚБЖ-ін іске асыруға және пайдалануға басшылардан рұқсат алуға.

к) Қолдану туралы Ережені дайындау.

Өзіне мына төмендегілер кіретін қолдану туралы Ереже дайындалуға тиіс:

1) 4.2.1ж) таңдап алынған басқару мақсаттары және басқару құралдары, сондай-ақ оларды таңдап алу себептері;

2) Осы сәтте іске асырылған басқару мақсаттары және басқару құралдары (4.2.1д)2) қараңыз);

3) А қосымшасында аталған басқарудың кез келген мақсаттарынан және басқарудың кез келген құралдарынан шығару, сондай-ақ осы мақсаттар мен құралдардың шығарылымдарына негіздеме.

Ескертпе – Қолдану туралы Ереже тәуекелдерді өңдеуге қатысты шешімдер ақпарын береді. Шығаруларды негіздеу басқарудың бір де бір құралы байқаусыздықтан жіберіліп алмағандығына айқас бақылауды қамтамасыз етеді.

4.2.2 АҚБЖ іске асыру және пайдалану

Ұйым мыналарды орындауға тиіс:

а) Ақпараттық қауіпсіздіктің тәуекелдерін басқару үшін басшылықтың тиісті әрекеттері, ресурстар, міндеттері және артықшылықтары сәйкестендірілетін тәуекелдерді өңдеу жоспарының ережелерін қалыптастыру (5-қараңыз).

б) Өзіне қаржыландыру, рөлдерді және жауапкершіліктерді үлестіру мәселелерін қарастыру кіретін сәйкестендірілген басқару мақсаттарына жету үшін тәуекелдерді өңдеу жоспарын іске асыру.

в) Басқару мақсаттарын орындау үшін 4.2.1ж) таңдап алынған басқару құралдарын іске асыру.

г) Таңдап алынған басқару құралдарының немесе басқару құралдарының топтарының тиімділігін қалай өлшеуге болатындығын айқындау және алынған нәтижелер салыстыруға келетіндей және

жаңғыртуға болатындай басқару құралдарының тиімділігін бағалау үшін осы өлшемдер қалай пайдалануға тиістігін көрсету (4.2.3в) қараңыз).

Ескертпе – Басқару құралдарының тиімділігін өлшеу менеджерлер мен қызметкерлерге басқару құралдары қаншалықты басқарудың жоспарланған мақсаттарына сәтті жететіндігін айқындауға жағдай жасайды.

д) Оқыту және жария ету бағдарламаларын іске асыру (5.2.2 қараңыз).

е) АҚБЖ пайдалануды басқару.

ж) АҚБЖ үшін ресурстарды басқару (5.2 қараңыз).

з) Қауіпсіздік оқиғаларын тез арада табуды және қауіпсіздіктің оқыс оқиғаларын сезінуді қамтамасыз етуге жағдай жасайтын рәсімдерді және басқарудың басқа құралдарын іске асыру (4.2.3а) қараңыз).

4.2.3 АҚБЖ мониторингі және талдау

Ұйым мыналарды орындауға тиіс:

а) мына мақсатта мониторинг рәсімдерін және рәсімдерді талдауды және басқа басқару құралдарын орындауға тиіс:

1) өңдеу нәтижелерінен қателерді дер кезінде табу;

2) қауіпсіздікті сәтсіз және сәтті бұзудың және қауіпсіздіктің оқыс оқиғаларын дер кезінде сәйкестендіру;

3) адамдарға тапсырылған немесе ақпараттық технологиялар құралдарымен іске асырылған қауіпсіздікті қамтамасыз ету бойынша әрекеттер тиісті жолмен орындалуда ма, соны басшылықтың айқындауына мүмкіндік беру;

4) қауіпсіздік оқиғаларын табуға көмектесу және міне осылай индикаторларды пайдалану жолымен қауіпсіздіктің оқыс оқиғаларын болдырмау;

5) қауіпсіздіктің бұзылуын жою үшін қамданған әрекеттер тиімді ме, соны айқындау.

б) Барлық мүдделі тараптардан алынған ұсыныстар мен ақпараттарды, тиімділікті өлшеу нәтижелерін, оқыс оқиғаларды, қауіпсіздікке аудиттің нәтижелерін ескере отырып, (АҚБЖ саясатын және қауіпсіздік мақсаттарын сақтау, сондай-ақ қауіпсіздікті басқару құралдарына талдауды қоса алғанда) АҚБЖ тиімділігіне жүйелі түрде талдауды жүзеге асыру.

в) Қауіпсіздік талаптары қанағаттандырылғанына көз жеткізу үшін басқару құралдарының тиімділігін өлшеу.

г) Жоспарланған кезеңдер арқылы тәуекелдерді бағалауға талдауды жүзеге асыру және қалған тәуекелдің деңгейін және мыналарда өтетін өзгерістерді ескере отырып, тәуекелдердің құптауға лайық сәйкестендірілген деңгейіне талдау жүргізу:

1) ұйымдар;

2) технологиялар;

3) бизнес-мақсаттар және бизнес-процесстерде;

4) сәйкестендірілген қауіп-қатерлерде;

5) басқарудың іске асырылған құралдарының тиімділігінде;

6) құқықтық немесе нормативтік саласындағы өзгерістер, шарттық міндеттемелердегі өзгерістер және қоғамдық климаттағы өзгерістер сияқты сыртқы оқиғаларда.

д) Жоспарланған кезеңдер арқылы АҚБЖ ішкі аудитін жүргізу (6-қараңыз).

Ескертпе – Кейде бірінші тарап аудиттері деп аталатын ішкі аудиттер ұйымның өзінің күшімен немесе ішкі мақсаттар үшін ұйымның тапсырысы бойынша орындалады.

е) Қолдану саласы бірдей күйінде қалатынына, ал АҚБЖ процессін жетілдіру сәйкестендірілгеніне кепілдік беру үшін басқарушы қызметкерлермен АҚБЖ-не жүйелі түрде талдау жүргізу (7.1 қараңыз).

ж) Мониторинг және талдау нәтижесінде алынған мәліметтерді ескеру үшін қауіпсіздік бойынша жоспарларды жаңару.

з) АҚБЖ өнімділігіне немесе тиімділігіне әсер етуі мүмкін әрекеттер мен оқиғаларды тіркеу (4.3.3 қараңыз).

4.2.4 АҚБЖ ілестіру және жетілдіру

Ұйым мыналарды жүйелі түрде орындауға тиіс:

а) АҚБЖ сәйкестендірілген жетілдіруді іске асыруды.

б) 8.2 және 8.3 тармақтарына сәйкес тиісті түзетуші және ескертпе шараларын қолдану. Басқа ұйымдарда бар, сондай-ақ ұйымның өзінде де бар қауіпсіздікті қамтамасыз ету тәжірибесінен алынған білімді қолдану.

в) Егер осыны әрекеттердің мәнділігі және маңыздылығы талап ететін болса, шаралар және жетілдірулер туралы (хабардың толықтық деңгейі жағдайларға сәйкес келуге тиіс) барлық тараптарды хабардар ету.

г) Жетілдіру қойылған мақсаттарға жететіндігіне көз жеткізу.

4.3 Құжаттамаға қойылатын талаптар

4.3.1 Жалпы талаптар

Құжаттамалар өзіне басқарушы шешімдердің жазбаларын кіргізуге тиіс, басқарушының шешімдері және саясаттарымен әрекеттердің байланысының бақыланып тұруына кепілдік беруге, сондай-ақ жазылған нәтижелердің жаңғыртылуын қамтамасыз етуге тиіс.

Таңдап алынған басқару құралдарынан кейін тәуекелдерді бағалау және тәуекелдерді өңдеу процесстерінің нәтижелеріне және одан әрі АҚБЖ саясаты және мақсаттарына дейінгі өзара байланысты көрсету мүмкіндігі болғаны маңызды.

АҚБЖ бойынша құжаттамаға мыналар кіруге тиіс:

а) қауіпсіздік саясатының (4.2.1б) қараңыз) және басқару мақсаттарының құжаттандырылған ережелері;

б) АҚБЖ қолдану саласы (4.2.1а) қараңыз);

в) АҚБЖ қолдау үшін пайдаланылатын рәсімдер және басқару құралдары;

г) тәуекелдерді бағалау әдістері туралы шешім (4.2.1в) қараңыз);

д) тәуекелдерді бағалау туралы есеп (4.2.1в) - 4.2.1ж) қараңыз);

е) тәуекелдерді өңдеу жоспары (4.2.2б) қараңыз);

ж) өзінің ақпараттық қауіпсіздік процесстерін тиімді жоспарлау, пайдалану және басқаруды қамтамасыз ету үшін және басқару құралдарының тиімділігі өлшеу әдістерін сипаттау үшін ұйымға қажетті құжаттандырылған рәсімдер (4.2.3в) қараңыз);

з) осы стандартпен талап етілетін жазбалар (4.3.3 қараңыз).

и) Қолдану туралы Ереже.

Ескертпе 1 – Осы стандартта «құжаттандырылған рәсім» термині осы рәсімнің әзірленгенін, құжаттандырылғанын, іске асырылғанын және қолдау алғанын білдіреді.

Ескертпе 2 – АҚБЖ бойынша құжаттамалар көлемі мыналарға байланысты бір ұйымнан екінші ұйым арасында:

1) Ұйымның мөлшері және оның қызмет түрлеріне;

2) қауіпсіздікке және басқару жүйесіне талаптардың күрделілігіне және қолдану салаларына байланысты өзгешеленуі мүмкін.

Ескертпе 3 – Құжаттар мен жазбалар кез келген тұрпаттағы тасымалдаушыда болуы мүмкін.

4.3.2 Құжаттарды басқару

АҚБЖ үшін қажетті құжаттар қорғалған және басқарылатын болуға тиіс. Мыналар үшін қажетті басқарылатын әрекеттерді айқындау үшін құжаттандырылған рәсім әзірленуге тиіс:

а) құжаттарды жариялау алдында олардың бірдейлік критерийлері бойынша құжаттарды бекіту;

б) қажеттілігіне қарай және құжаттарды қайтадан бекіту бойынша құжаттарды талдау және жаңарту;

в) құжаттардың ағымдағы редакциясының мәртебесін және өзгертулерді сәйкестендіруді қамтамасыз ету;

г) тиісті құжаттардың маңызды нұсқаларына оларды пайдалану жерлерінде қол жетімдікпен қамтамасыз ету;

д) құжаттардың тез сәйкестендіруін және жеңіл оқылатындығын сақтау;

е) оларды талап ететіндер үшін құжаттарға қол жетімдікті қамтамасыз ету, сондай-ақ құжаттар жіктемесіне сәйкес қолданылатын рәсімдерге сәйкес табыстау, сақтау және ақырында құжаттарды жоюды қамтамасыз ету.

ж) сырттан шыққан құжаттарды сәйкестендірумен қамтамасыз ету;

з) құжаттарды таратуға бақылауды қамтамасыз ету;

и) ескірген құжаттарды кездейсоқ пайдалануды болдырмау;

к) егер олар қандай да бір мақсаттар үшін сақталатын болса, құжаттарды қолайлы сәйкестендіруді қолдану.

4.3.3 Жазбаларды басқару

АҚБЖ тиімді пайдалану және талаптарына сәйкестік куәлігін қамтамасыз ететін жазбалар жасалуға және қолдануға тиіс. Жазбалар қорғалған және басқарылатын болуға тиіс. АҚБЖ барлық маңызды құқықтық және нормативтік талаптарды, сондай-ақ шарттық міндеттемелерді ескеруге тиіс. Жазбалар жеңіл оқылатын, оңай сәйкестендірілетін және шығарылатын болуға тиіс. Жазбаларды сәйкестендіру, сақтау, қорғау, шығару және жою үшін қажет, сондай-ақ жазбалардың сақталу мерзімі құжаттандырылуға және іске асырылуға тиіс.

4.2 тармақта сипатталғандай процесстің өнімділігінің жазбасы және АҚБЖ-мен байланысты қауіпсіздіктің маңызды оқыс оқиғалар жағдайларының жазбалары жүргізілуге тиіс.

Мысал-Қатысу журналы, аудит туралы есептер және қатынауға рұқсаттың толтырылған нышандары жазбалардың мысалдары болып табылады.

5 Қызметкерлердің міндеттерін тарату

5.1 Басшылықтың мүдделілігі

Басшылар мыналар арқылы АҚБЖ әзірленіміне, іске асыруға, пайдалануға, мониторингке, талдауға, алып жүруге және жетілдіруге өздерінің мүдделілігін көрсетуге тиіс:

а) АҚБЖ саясатын бекіту;

б) АҚБЖ мақсаттары мен жоспарлары айқындалғанын куәландыру.

в) ақпараттық қауіпсіздік үшін рөлдер мен жауапкершіліктерді бекіту;

г) ақпараттық қауіпсіздіктің мақсаттарына жету және ақпараттық қауіпсіздіктің саясатын сақтау, заң алдында ұйымның жауапкершілігі және үздіксіз жетілдіру қажеттігінің маңыздылығы туралы ұйымды хабардар ету;

д) АҚБЖ әзірлеу, іске асыру, пайдалану, алып жүру және жетілдіру үшін жеткілікті түрде ресурстар беру (5.2.1 тармағын қараңыз);

е) тәуекелдерді және тәуекелдердің құптауға лайық деңгейлерін қабылдау үшін критерийлерді таңдау;

ж) АҚБЖ-нің ішкі аудиттарын өткізуді қамтамасыз ету (6 тармақты қараңыз);

з) АҚБЖ-не басқарушылық талдау жүргізу (7 тармағын қараңыз).

5.2 Ресурстарды басқару

5.2.1 Ресурстарды беру

Ұйым мыналар үшін қажетті ресурстарды айқындауға және беруге тиіс:

а) АҚБЖ әзірлеу, іске асыру, пайдалану, мониторинг, талдау, алып жүру және жетілдіру үшін;

б) ақпараттық қауіпсіздік рәсімдерімен бизнес-талаптарды қолдауды қамтамасыз ету үшін;

в) құқықтық және нормативтік талаптарды, сондай-ақ қауіпсіздік бойынша шарттық міндеттемелерді сәйкестендіру және есепке алу;

г) барлық іске асырылған басқару құралдарын дұрыс қолдану көмегімен ұқсас қауіпсіздікті қамтамасыз ету;

д) талдау нәтижелері бойынша қажеттілігіне қарай және тиісті әсер етуге қарай талдауды орындау;

е) егер талап етілетін болса, АҚБЖ тиімділігін жетілдіру.

5.2.2 Оқыту, мәліметтілік және біліктілік

Ұйым АҚБЖ-де айқындалған міндеттер жүктелген барлық қызметкердің қажетті міндеттерді орындау үшін тиісті біліктілігі болуға кепілдік беруге тиіс. Бұл үшін ұйым:

а) АҚБЖ-мен байланысты жұмыстарды орындайтын қызметкердің біліктілігінің қажетті деңгейін айқындауға тиіс;

б) оқытуды қамтамасыз етуге немесе осы қажеттіліктерді қанағаттандыру үшін басқа шараларды (мысалы, білікті қызметкерлерді қабылдауға) қолдануға тиіс;

в) қабылданған шаралардың тиімділігін бағалауға тиіс;

г) білім беру, оқыту, дағдылар, тәжірибе және біліктілік туралы жазба жүргізуге (4.3.3-тармағын қараңыз).

Ұйым, сондай-ақ бүкіл қызметкерлердің ақпараттық қауіпсіздікті қамтамасыз ету бойынша оның қызметінің мәнділігі және маңыздылығы туралы хабардар болуына, сондай-ақ АҚБЖ-нің мақсаттарына жетуде осы қызметкер қандай жолмен қатысатындығына кепілдік беруге тиіс.

6 АҚБЖ ішкі аудиттері

Мынадай қасиеттерімен АҚБЖ-нің рәсімдері және процесстері, басқару мақсаттары, басқару құралдарына ие ме, соны айқындау үшін ұйым жоспарланған уақыт аралықтары арқылы АҚБЖ-нің ішкі аудитін жүргізуге тиіс:

а) осы стандарттың және тиісті заңдар және нормативтердің талаптарын қанағаттандырады;

б) ақпараттық қауіпсіздіктің сәйкестендірілген талаптарын қанағаттандырады;

в) тиімді іске асырылған және алып жүрген болып табылады;

г) күтуге сәйкес орындалады.

Аудиттің бағдарламасы аудит жүргізуге жататын процесстер мен салалардың мәртебесі мен маңыздылығын ескере отырып, сондай-ақ

алдыңғы аудиттардың нәтижелерін ескере отырып, жоспарлануға тиіс. Аудиттің критерийлері, шекаралары, кезеңділігі және әдістері айқындалуға тиіс. Аудиторларды таңдау және аудит жүргізуде аудит процессінің шынайылығына және әділдігіне кепілдік беруге тиіс. Аудиторлар өзінің жеке жұмысына аудит жүргізбеуге тиіс.

Аудитті жоспарлауға және өткізуге, сондай-ақ аудитті өткізу нәтижелері бойынша есептемеге және жазбалар жүргізуге міндеттер және талаптар (4.3.3 тармағын қараңыз) құжаттандырылған рәсімде айқындалуға тиіс.

Аудитке жататын сала үшін жауапты басқарушы қызметкер табылған сәйкессіздіктерді және олардың себептерін жою үшін тез арада шаралар қабылдануын қамтамасыз етуге тиіс. Әрі қарайғы әрекеттердің өзіне қолданылған шараларды тексеру және тексеру нәтижелері бойынша есеп кіргізілуге тиіс (8-тармақты қараңыз).

Ескертпе – ISO 19011:2002, Guidelines for quality and/or environmental management systems стандартында АҚБЖ ішкі аудиттерін өткізу жөніндегі пайдалы нұсқау бар.

7 Басшылықтың АҚБЖ қайта қарауы

7.1 Жалпы ережелер

Басқарушы қызметкер жоспарланған аралық арқылы (жылына бір рет) АҚБЖ-нің үздіксіз қолданылуын, барабарлығын және тиімділігін қамтамасыз ету үшін ұйымның АҚБЖ-іне талдау жасауға тиіс. Бұл талдау өзіне АҚБЖ-ін, соның ішінде ақпараттық қауіпсіздік саясатын және ақпараттық қауіпсіздік мақсаттарын жетілдіру мүмкіндіктерін және өзгерту қажеттілігін айқындауды кіргізуге тиіс. Талдау нәтижелері нақты түрде құжаттандырылуға тиіс, сондай-ақ тиісті жазбалар жүргізілуге тиіс (4.3.3-тармағын қараңыз).

7.2 Талдау үшін бастапқы деректер

Басқарушылық талдауы үшін бастапқы деректерге мыналар кіруге тиіс:

а) АҚБЖ-нің аудиттер және талдау нәтижелері;

б) мүдделі тараптардың ескертпелері мен ұсыныстары;

в) АҚБЖ өнімділігін және тиімділігін арттыру үшін ұйымда пайдалану болатын әдістер, өнімдер немесе рәсімдер туралы ақпарат;

г) ескертпе беруші және түзетуші шаралардың мәртебесі туралы ақпарат;

д) тәуекелдерді алдыңғы бағалау кезінде барабар ескерілмеген қауіп-қатерлер немесе осалдықтар туралы ақпарат;

е) тиімділікті өлшеу нәтижелері;

ж) алдыңғы басқарылатын талдаудың нәтижелері бойынша қолданылған шаралар туралы ақпарат;

з) АҚБЖ-не әсер етуі мүмкін барлық өзгерістер туралы ақпарат;

и) жетілдіру жөніндегі ұсыныстар.

7.3 Талдау қорытындылары

Басқарылатын талдаудың қорытындыларының өзіне төменде аталғандармен байланысты барлық шешімдер мен шаралар кіргізілуге тиіс.

а) АҚБЖ-нің тиімділігін арттыру.

б) Тәуекелдерді бағалауды және тәуекелдерді өңдеу жоспарын жаңарту.

в) Мыналарға өзгертулерді қоса алғанда, АҚБЖ-не әсер етуі мүмкін ішкі және сыртқы оқиғаларды сезіну үшін, ақпараттық қауіпсіздікке әсер ететін рәсімдер мен басқару құралдарын қажеттілігіне қарай түрлендіру:

1) бизнес-талаптарға;

2) қауіпсіздік талаптарына;

3) қолданыстағы бизнес-талаптарға әсер ететін бизнес-процесстерге;

4) нормативтік немесе құқықтық талаптарға;

5) шарттық міндеттемелерге;

6) тәуекелдер деңгейлеріне және/немесе тәуекелдерді қабылдау критерийлеріне.

г) Ресурстарға қажеттілікті айқындау.

д) Басқару құралдарының тиімділігін өлшеудің қолданыстағы әдістерін жетілдіру.

8 АҚБЖ жетілдіру

8.1 Үздіксіз жетілдіру

Ұйым ақпараттық қауіпсіздік саясатын, ақпараттық қауіпсіздік мақсаттарын, аудит нәтижелерін, бақыланған оқиғалардың талдауын, түзетуші және ескертпе беруші әсер етулерді, сондай-ақ басқарылатын талдауды пайдалану жолымен АҚБЖ-нің тиімділігін үздіксіз арттырып отыруға тиіс (7-тармағын қараңыз).

8.2 Түзетушілік әсер ету

Ұйым сәйкессіздіктердің қайталанып пайда болуын болдырмау үшін АҚБЖ-нің талаптарына сәйкессіздіктерді жою үшін шаралар қолдануға тиіс. Түзетушілік әсер ету үшін құжаттандырылған рәсім мыналарға талаптарды айқындауға тиіс:

а) сәйкессіздіктерді сәйкестендіруге;

б) сәйкессіздіктердің себептерін айқындауға;

в) сәйкессіздіктің қайталап пайда болуын болдырмайтын әсер етудің қажеттілігін бағалауға;

г) қажетті түзетушілік әсер етуді айқындау және іске асыру;

д) қолданылған әсер ету нәтижелерін тіркеу (4.3.3-тармағын қараңыз);

е) жасалған түзетушілік әсер етудің талдауына.

8.3 Ескертпешілік әсер ету

Ұйым сәйкессіздіктің пайда болуын болдырмау үшін АҚБЖ-інің талаптарына ықтимал сәйкессіздіктердің себебін болдырмау үшін шараларды айқындауға тиіс. Жасалған ескертпешілік шаралар әлуетті мәселелерге әсер етумен барабар болуға тиіс. Ескертпешілік әсер ету үшін құжаттандырылған рәсім мыналарға талаптарды айқындауға тиіс:

а) әлуетті сәйкессіздіктерді және олардың себептерін сәйкестендіруге;

б) сәйкессіздіктің пайда болуын болдырмау үшін әсер етудің қажеттігін бағалауға;

в) қажетті ескертпешілік әсер етуді айқындау және іске асыру;

г) жасалған әсер ету нәтижелерін тіркеуге (4.3.3-тармағын қараңыз);

д) жасалған ескертпешілік әсер етудің талдауына.

Ұйым елеулі өзгерген тәуекелдерге ерекше назар аудара отырып, ескертпешілік әсер етуге талаптарды сәйкестендіруге және өзгерген тәуекелдерді сәйкестендіруге тиіс.

Ескертпешілік әсер етудің артықшылығы тәуекелдерді бағалау нәтижелерінің негізінде айқындалуға тиіс.

Ескертпе – Сәйкессіздіктерді болдырмау бойынша әрекет, түзетуші әсер етуге қарағанда қымбатырақ болып табылады.

А қосымшасы
(ұсынылатын)
Басқару мақсаттары және басқару құралдары

А.1-кестесінде аталған басқару мақсаттары және басқару құралдары, тікелей ISO/IEC 17799:2005 стандартының **5-тен бастап 15-ке дейінгі** тармақтарында аталған мақсаттар мен құралдардан алынған және соларға сәйкес болады. А.1-кестедегі тізімдер соңғы болып табылмайды және ұйым қосымша басқару мақсаттары мен басқару құралдарын пайдалану қажет деп санауы мүмкін. Осы кестелердегі басқару мақсаттары және басқару құралдары **4.2.1**-тармағында айқындалған АҚБЖ процессінің бір бөлігі ретінде таңдап алынуға тиіс.

ISO/IEC 17799:2005 стандартының **5–15**-тармақтарында **А.5**–**А.15**-тармақтарында сипатталған басқару құралдарын практикалық қолдану жөнінде нұсқау және іске асыру жөніндегі кеңестер бар.

А.1-кесте – Басқару мақсаттары және басқару құралдары

А.5 Қауіпсіздік саясаты		
А.5.1 Ақпараттық қауіпсіздік саясаты Мақсаты: Бизнес-талаптарға және тиісті заңдар мен нормативтерге сәйкес басқарушы қызметкерлер тарапынан ақпараттық қауіпсіздік үшін басқару және қолдауды қамтамасыз ету.		
А.5.1.1	Ақпараттық қауіпсіздік саясаты туралы құжат	Басқару құралдары Ақпараттық қауіпсіздік саясаты туралы құжат ұйымның басшылығымен бекітілуге, жариялануға және сыртқы релеванттық тараптарға және барлық қызметкерлерге дейін жеткізілуге тиіс.
А.5.1.2	Ақпараттық қауіпсіздік саясатын талдау	Басқару құралдары Ақпараттық қауіпсіздік саясаты жоспарланған аралықтар арқылы немесе елеулі өзгерістер пайда болған жағдайда, оның үздіксіз қолданушылығын, барабарлығын және тиімділігін қамтамасыз ету үшін талдануға тиіс.
А.6 Ақпараттық қауіпсіздіктің ұйымдастыру аспектілері		
А.6.1 Ішкі ұйымдастыру аспектілері Мақсаты: Ұйымдағы ақпараттық қауіпсіздікті басқару.		
А.6.1.1	Басшылардың ақпараттық қауіпсіздікке мүдделілігі	Басқару құралдары Басшылар тікелей нұсқау, мүдделілікті көрсету, тікелей тағайындау және ақпараттық қауіпсіздік үшін жауапкершілікті мақұлдау жолымен ұйымдағы қауіпсіздікті белсенді қолдауға тиіс.
А.6.1.2	Ақпараттық қауіпсіздікті үйлестіру	Басқару құралдары Ақпараттық қауіпсіздік бойынша қызмет тиісті рөлдер және жұмыс қызметтерімен ұйымның әр түрлі бөліктерінің өкілдерімен үйлестірілуге тиіс.

A.6.1.3	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша міндеттерді үлестіру	Басқару құралдары Ақпараттық қауіпсіздікті қамтамасыз ету бойынша міндеттер нақты айқындалуға тиіс.
A.6.1.4	Ақпаратты өңдеу құралдарын бекіту процессі	Басқару құралдары Жаңа өңдеу құралдарын басшылардың бекіту процессі айқындалуға және іске асырылуға тиіс.
A.6.1.5	Құпиялық туралы келісім	Ақпаратты қорғауға ұйымның қажеттілігін көрсететін жарияламау немесе құпиялық туралы келісімдерге талаптар жүйелі түрде қайта қаралуға және сәйкестендірілуге тиіс.
A.6.1.6	Уәкілетті ұйымдармен байланыс	Басқару құралдары Тиісті ұйымдармен тиісті байланыстар үзілмеуге тиіс.
A.6.1.7	Мамандандырылған топтармен байланыс	Басқару құралдары Ақпараттық қауіпсіздік және кәсіби бірлестіктер бойынша мамандандырылған топтармен және мамандардың басқа форумдарымен тиісті байланыс үзілмеуге тиіс.
A.6.1.8	Ақпараттық қауіпсіздікті тәуелсіз талдау	Басқару құралдары Ақпараттық қауіпсіздікті басқару және іске асыруға ұйымның тәсілі (яғни ақпараттық қауіпсіздікті басқару мақсаттары, басқару құралдары, саясаты, процесстері және рәсімдері) жоспарланған уақыт аралықтары арқылы немесе қауіпсіздікті іске асыруда елеулі өзгерістер болған жағдайда тәуелсіз талдауға ұшырауға тиіс.
A.6.2 Сыртқы ұйымдастыру аспекттері Мақсаты: Қол жететін, өңделіп жатқан, белгілі немесе басқа ұйымдармен басқарылатын ұйымның ақпаратын өңдеу құралдарын және ақпараттың қауіпсіздігін қамтамасыз ету.		
A.6.2.1	Шеттегі ұйымдармен байланысты тәуекелдерді сәйкестендіру	Басқару құралдары Сыртқы ұйымдар тартылған бизнес-процесстерде туындайтын ұйымның ақпаратын өңдеу жүйесі және ақпараты үшін тәуекелдер, сәйкестендірілуге тиіс және осы ақпарат және құралдарға рұқсат берілгенге дейін басқаруды тиісті құралдары іске асырылуға тиіс.
A.6.2.2	Тапсырыс берушілермен келісімдердегі қауіпсіздікті қамтамасыз ету	Басқару құралдары Қауіпсіздіктің барлық сәйкестендірілген талаптары тапсырыс берушілерге ұйымның ақпараттарына немесе ресурстарына рұқсат берілгенге дейін орындалуға тиіс.
A.6.2.3	Шеттегі ұйымдармен келісімдердегі қауіпсіздікті қамтамасыз ету	Басқару құралдары Ұйымның ақпаратын өңдеу құралдарын немесе ақпаратын басқару, қатынау, өңдеу, пайдалануды не болмаса өнімдерді немесе сервисті ақпаратты өңдеу құралдарына қосуды көздейтін шеттегі ұйымдармен келісімдер, келісім мәніне жататын қауіпсіздіктің барлық талаптарын ескеруге тиіс.
A.7 Ресурстарды басқару		
A.7.1 Ресурстар үшін жауапкершілік Мақсаты: Ұйымның ресурстарын тиісті қорғауды қолдау және қамтамасыз ету.		

А.7.1.1	Ресурстарды түгендеу	Басқару құралдары Барлық ресурстар нақты сәйкестендірілуге тиіс, барлық маңызды ресурстардың тізімі жасалуға және маңызды жағдайда ұсталуға тиіс.
А.7.1.2	Ресурстарға ие болу	Басқару құралдары Ақпаратты өңдеу құралдарымен байланысты барлық ақпарат және ресурстар, ұйымның уәкілетті бөлімшесінің «иелігінде» [2] болуға тиіс.
А.7.1.3	Рұқсат берілген ресурстарды пайдалану	Басқару құралдары Ақпаратты өңдеу құралдарымен байланысты ақпараттар және ресурстарды жорамалды пайдалану ережесі сәйкестендірілуге, құжаттандырылуға және іске асырылуға тиіс.
А.7.2 Ақпаратты жіктеу Мақсаты: Ақпаратты қорғаудың тиісті деңгейінің қамтамасыз етілгеніне кепілдік беру.		
А.7.2.1	Жіктеу бойынша ұсыныстар	Басқару құралдары Ақпарат мәнділік, құқықтық талаптар, әсер етулерге сезімталдық және ұйым үшін сыншылдық сияқты көрсеткіштер бойынша жіктелуге тиіс.
А.7.2.2	Ақпаратты таңбалау және ұстау	Басқару құралдары Ақпаратты ұстау және таңбалау үшін ұйымда қабылданған жіктеме жүйесіне сәйкес тиісті рәсімдер жинағы әзірленуге және іске асырылуға тиіс.
А.8 Қызметкерлермен байланысты қауіпсіздік аспектілері		
А.8.1 Жұмысқа дейін[3] Мақсаты: Шеттегі ұйымдардың қызметкерлері, мердігерлері және пайдаланушылары өз жауапкершілігін түсінетініне және оларға арналған рөлдерге лайықты екеніне, сондай-ақ жабдықтарды ұрлау, алаяқтық немесе дұрыс пайдаланбау тәуекелін азайтуға кепілдік беру.		
А.8.1.1	Рөлдер және жауапкершілік салалары	Басқару құралдары Шеттегі ұйымдардың қызметкерлерінің, мердігерлерінің және пайдаланушыларының қауіпсіздік рөлдері және жауапкершілігі ұйымның ақпараттық қауіпсіздік саясатына сәйкес айқындалуға тиіс.
А.8.1.2	Жұмысқа қабылданушыларды тексеру	Басқару құралдары Шеттегі ұйымдардың бос орынға кандидаттардың барлығының, мердігерлердің және пайдаланушылардың жеке деректерін тексеру тиісті заңдарға, нормативтік құжаттарға және этикалық нормаларға сәйкес, сондай-ақ рұқсат берілетін және тәуекелдермен түсінілетін бизнес-талаптарды, ақпараттар санатын ескере отырып, орындалуға тиіс.

[2] Түсіндірме: «Иегер» (owner) термині осы ресурстардың тиімділігін (production), дамуын, алып жүру, пайдалану және қауіпсіздігін басқару үшін әкімшілік жауапкершілік жүктелген тұлғаны немесе мәнді білдіреді. «Иегер» термині осы ресурсқа осы тұлғаның қандай да бір меншік құқығы бар дегенді білдірмейді.

[3] Түсіндірме: «жалдау» ('employment') термині мынадай барлық жағдайларды: қызметкерлерді жалдау (уақытша немесе тұрақты), жұмысшы рөлдерді тағайындау, жұмыс рөлдерін өзгерту, келісім-шарттарды қайта табыстау (assignment of contracts), аталған келісімдердің кез келгенінің мерзімінің аяқталуын белгілеу үшін мұнда пайдаланылады.

А.8.1.3	Жалдау қаулысы және шарттары	Басқару құралдары Шеттегі ұйымдардың қызметкерлері, мердігерлері және пайдаланушылары өздерінің келісім-шарттық міндеттемелерінің бір бөлігі ретінде ақпараттық қауіпсіздік үшін ұйымның жауапкершілігін және олардың жауапкершілігін белгілеуге тиіс, жалдау туралы өзінің келісім-шартының қаулысына және ережесіне қол қоюға және қабылдауға тиіс.
А.8.2 Жалдау кезінде Мақсаты: Шеттегі ұйымдардың қызметкерлері, мердігерлері және пайдаланушылары өздерінің әдеттегі жұмыс процессінде ұйымның қауіпсіздік саясатын ұстауға қабілетті, өзінің міндеттемелері мен жауапкершілігі туралы, оның мәні және ақпараттық қауіпсіздікке қауіп-қатер туралы хабардар екеніне кепілдік беру.		
А.8.2.1	Басшылардың жауапкершілігі	Басқару құралдары Басшылар шеттегі ұйымдардың қызметкерлері, мердігерлері және пайдаланушылары ұйымда белгіленген саясаттар мен рәсімдерге сәйкес ақпараттық қауіпсіздіктің ережесінің қолданылуын талап етуге тиіс.
А.8.2.2	Ақпараттық қауіпсіздік саласындағы мәліметтілік, оқыту және біліктілік	Басқару құралдары Шеттегі ұйымдардан мердігерлер және пайдаланушылар қажет ұйымның барлық қызметкерлері олардың өздерінің жұмыс қызметтерін орындау үшін қажет көлемде ұйымның саясаты және рәсімдерін жаңарту туралы ақпаратты жүйелі түрде алуға және тиісті мәліметтілік беретін оқыту алуға тиіс.
А.8.2.3	Тәртіптік іс	Басқару құралдары Қауіпсіздікті бұзған қызметкерлер үшін заңға сәйкес тәртіптік іс айқындалуға тиіс.
А.8.3 Жұмыстан босату немесе жалдау шартын өзгерту Мақсаты: Шеттегі ұйымдардың қызметкерлері, мердігерлері және пайдаланушылары ұйымнан кетеді немесе белгіленген тәртіпте жалдау шартын өзгертетініне кепілдік беру.		
А.8.3.1	Жұмыстан босату үшін жауапкершілік	Басқару құралдары Қызметкерлерді жұмыстан босату рәсімін орындағаны үшін немесе жалдау шартын өзгерту үшін жауапкершілік айқындалуға және тағайындалуға тиіс.
А.8.3.2	Ресурстарды қайтару	Басқару құралдары Шеттегі ұйымдардың барлық қызметкерлері, мердігерлері және пайдаланушылары келісім шарттың (келісімдердің) әрекет ету мерзімі аяқталу немесе жұмыстан босату күніне дейін, олардың билігіндегі барлық ресурстарды қайтаруға тиіс.
А.8.3.3	Қол жеткізу құқығын тоқтату	Басқару құралдары Шеттегі ұйымдардың барлық қызметкерлерінің, мердігерлерінің және пайдаланушыларының ақпаратқа және ақпаратты өңдеу құралдарына қол жетушілік құқығы жұмыстан босатылған, келісім-шартты немесе келісімді тоқтатқан жағдайда не жойылуға не болмаса жалдаудың шарттарын өзгертуге сәйкес өзгертілуге тиіс.
А. 9 Физикалық қауіпсіздік және қызмет істеу ортасының қауіпсіздігі		
А.9.1 Қорғалатын салалар Мақсаты: Ұйымның аумағына, жабдығына және ақпаратына санкцияланбаған физикалық қол жетушілік, залал немесе әсерді болдырмау.		

А.9.1.1	Қауіпсіздіктің физикалық периметрі	Басқару құралдары Ақпарат және ақпаратты өңдеу құралдары орналасқан салаларды қорғау үшін қауіпсіздіктің периметрлері пайдаланылуға тиіс (карталар бойынша жіберу жүйесімен жабдықталған қабырға, кіріс сияқты барьерлер, немесе арнайы қызметкерлер кіретін бақылау).
А.9.1.2	Үй-жайға қол жеткізуді бақылау	Басқару құралдары Қорғалатын салалар тиісті өкілеттік алған қызметкер ғана оларға қол жетуін қамтамасыз ететін үй-жайға қатынаудың қажетті бақылау құралдарымен қорғалуға тиіс.
А.9.1.3	Кеңселерді, бөлмелерді және жабдықтарды қорғау	Басқару құралдары Кеңселерді, бөлмелерді және жабдықтарды қорғау үшін физикалық қауіпсіздік шаралары әзірленіп, енгізілуге тиіс.
А.9.1.4	Сыртқы қауіп-қатерден және қоршаған ортаның қауіп-қатерінен қорғау	Басқару құралдары Өрттен, су басудан, жер сілкінісінен, жарылыстардан, азаматтық ретсіздіктерден және табиғи және антропогендік апаттардың басқа нышандарынан физикалық қорғаудың шаралары әзірленіп, енгізілуге тиіс.
А.9.1.5	Қорғалған салалардағы жұмыс	Басқару құралдары Қорғалған облыстардағы жұмыс қағидалары және физикалық қорғау шаралары әзірленіп, енгізілуге тиіс.
А.9.1.6	Еркін қатынау, жүк тиеу және жүк түсіру орындары	Басқару құралдары Уәкілетті емес тұлғалардың қатынау мүмкіндігі бар жүк түсіру және жүк тиеу алаңшалары және басқа орындар сияқты еркін қатынау орындары бақылануға тиіс және мүмкіндігінше санкцияланбаған қатынауды болдырмау мақсаттарында ақпаратты өңдеу құралдарынан оқшауланған тиіс.
А.9.2 Жабдықтарды қорғау Мақсаты: Ресурстардың жоғалуын, зақымдануын, ұрлануын немесе компрометациясын, сондай-ақ ұйымның қызметіндегі іркілістерін болдырмау		
А.9.2.1	Жабдықтарды орналастыру және қорғау	Басқару құралдары Жабдық сыртқы ортаның әрекет етуімен, санкцияланбаған қатынау ықтималдығына байланысты тәуекел және залалды азайтатындай орналастырылуы немесе қорғалған болуға тиіс.
А.9.2.2	Көтермелеуші инфрақұрылым	Басқару құралдары Жабдық көтермелеуші инфрақұрылымдағы іркілістер үшін туындайтын электрмен қоректендіру жүйесіндегі іркілістер және басқа ақаулардан қорғалуға тиіс.
А.9.2.3	Кабель желісін қорғау	Басқару құралдары Деректерді беретін немесе ақпараттық қызметтерді қолдау үшін пайдаланылатын электрмен қоректендіру және телекоммуникациялардың кабельдік жүйесі, тыңдаудан немесе зақымданудан қорғалған болуға тиіс.
А.9.2.4	Жабдықтарды алып бару	Басқару құралдары Жабдықтардың үздіксіз қол жеткізуіне және бүтіндігіне кепілдік беру үшін оны тиісті алып барумен қамтамасыз етілуге тиіс.
А.9.2.5	Ұйымнан тысқары жабдықтардың қауіпсіздігі	Басқару құралдары Ұйымнан тысқары жабдықтарға ұйымның аумағынан тысқары жұмыстардың әр түрлі тәуекелдері ескерілетін қауіпсіздік шаралары қолданылуға тиіс.

А.9.2.6	Сенімді пайдаға асыру немесе жабдықты қайталап пайдалану	Басқару құралдары Пайдаға асыру алдында одан барлық деректер және лицензияланған бағдарламалық жабдықтамалар жойылғанына немесе басқа ақпаратпен сенімді алмастырылғанына кепілдік беру үшін, ақпаратты тасымалдаушылар бар жабдықтардың барлық бірліктері тексерілуге тиіс.
А.9.2.7	Меншікті ауыстыру	Басқару құралдары Жабдықтар, ақпараттар немесе бағдарламалық жабдықтамалар басшылардың тиісті санкциясыз ұйымнан тысқары шығарылмауға тиіс.
А.10 Коммуникацияларды және қызмет істеуін басқару		
А.10.1 Операциялық рәсімдер және жауапкершілік Мақсаты: Ақпаратты өңдеу құралдарының дұрыс және қорғалған қызмет істеуін қамтамасыз ету.		
А.10.1.1	Құжаттандырылған операциялық рәсімдер	Басқару құралдары Операциялық рәсімдер құжаттандырылуға тиіс, оларды алып бару, сондай-ақ олар талап етілетін барлық пайдаланушылар үшін қол жетімдікпен қамтамасыз етілуге тиіс.
А.10.1.2	Өзгертулерді басқару	Басқару құралдары Ақпаратты өңдеу жүйелерінде және құралдарындағы өзгерістер бақылануға тиіс.
А.10.1.3	Міндеттерді бөлу	Басқару құралдары Міндеттер және жауапкершілік аумағы санкцияланған немесе қасақана емес түрлендіру немесе ұйымның ресурстарын дұрыс пайдаланбау ықтималдығын азайту үшін бөлінуге тиіс.
А.10.1.4	Әзірленім, сынақ құралдарын және өндірістік құралдарын бөлу	Басқару құралдары Әзірленім, сынақ құралдары және өндірістік құралдары операциялық жүйенің өзгерістері немесе санкцияланбаған қатынау тәуекелін азайту үшін бөлінуге тиіс.
А.10.2 Шеткі ұйымдардың ұсынған қызметтерін басқару Мақсаты: Ақпараттық қауіпсіздіктің тиісті деңгейін іске асыру және қолдау және шеткі ұйымдарға қызмет көрсетулерді жеткізу туралы келісімге сәйкес қызметтерді ұсыну.		
А.10.2.1	Қызмет ұсыну	Басқару құралдары Шеттегі ұйымдармен сервистерді жеткізу туралы келісімге енгізілген қауіпсіздікті басқару құралдарының қызметтерін және жеткізу деңгейлерін айқындауға кепілдік берілуге тиіс, іске асырады, қызмет істейді және шеттегі ұйым алып жүреді.
А.10.2.2	Шеттегі ұйымдардың сервисі қадағалау (мониторинг) және талдау	Басқару құралдары Шеттегі ұйымдармен ұсынылатын сервистер, есептер және жазбалар, жүйелі түрде қадағалануға (мониторингке) және талдауға ұшырауға тиіс, одан басқа, жүйелі түрде аудит өткізілуге тиіс.
А.10.2.3	Шеттегі ұйымдардың қызметтеріндегі өзгерістерді басқару	Басқару құралдары Қолданыстағы ақпараттық қауіпсіздіктің саясатын алып жүру және жетілдіруді, басқару рәсімдері мен құралдарын қоса алғанда сервистерді ұсынудағы өзгертулер тартылған бизнес-жүйелер және процесстердің сыншылдығын, сондай-ақ тәуекелдерді қайталап бағалауды ескере отырып басқарылуға тиіс.

А.10.3 Жүйелерді жоспарлау, оларды қабылдау Мақсаты: Жүйелер іркілісінің тәуекелін азайту.		
А.10.3.1	Жүктемелерді жоспарлау	Басқару құралдары Ресурстарды пайдалану қадағалануға (мониторинг) және сәйкестікке келтірілуге тиіс, жүйенің қажетті өнімділігін қамтамасыз ету үшін болашақ қажеттіліктер болжамы жасалуға тиіс.
А.10.3.2	Жүйелерді қабылдау	Басқару құралдары Жаңа ақпараттық жүйелерді, жаңғыртуларды және жаңа нұсқаларды қабылдау критерийлері орнатылуға тиіс және жүйені қабылдағанға дейін, жүйені әзірлеген кезде тиісті сынақтан өткізу орындалуға тиіс.
А.10.4 Зиян келтіретін жедел әрекеттік бағдарламалық кодтан қорғау Мақсаты: Бағдарламалық жабдықтау және ақпараттың тұтастығын қамтамасыз ету.		
А.10.4.1	Зиян келтіретін бағдарламалық кодтан қорғау құралдары	Басқару құралдары Зиян келтіретін бағдарламалық кодтан қорғаныспен қамтамасыз ететін табу, болдырмау және қалпына келтіру құралдары, сондай-ақ пайдаланушыларды хабардар ететін тиісті рәсімдер іске асырылуға тиіс.
А.10.4.2	Жедел әрекеттік кодтан қорғау құралдары	Басқару құралдары Жедел әрекеттік код пайдалануға рұқсат етілген жерлерде, конфигурация санкцияланған жедел әрекеттік кодтың қауіпсіздіктің нақты берілген саясатына сәйкес қызмет істейтіндігіне кепілдік беруге тиіс, ал санкцияланбаған мобильдік кодтың орындалуына жол берілмейді.
А.10.5 Резервтік көшіру		
А.10.5.1	Ақпаратты резервтік көшіру	Басқару құралдары Ақпараттың және бағдарламалық жабдықтаманың резервтік көшірмелері резервтік көшіру саясатымен белгіленгенге сәйкес жүйелі түрде жасалуға және сынақтан өтуге тиіс.
А.10.6 Желілердің қауіпсіздігін басқару Мақсаты: Желілердегі ақпаратты қорғаумен және көтермелеуші инфрақұрылымдарды қорғаумен қамтамасыз ету.		
А.10.6.1	Желіні басқару құралдары	Басқару құралдары Желілер бойынша берілетін ақпаратты қоса алғанда, желімен пайдаланылатын қосымшалар және жүйелер қауіпсіздігін қолдау үшін және қауіп-қатерден қорғалған болу үшін тиісті жолмен басқарылуға және бақылануға тиіс.
А.10.6.2	Желілік қызметтердің қауіпсіздігі	Басқару құралдары Барлық желілік қызметтер үшін қауіпсіздік құралдары, қызметтер деңгейі және басқару бойынша талаптар сәйкестендірілуге тиіс және осы қызметтер ұйымның өзінің күшімен немесе сыртқы ұйымдардың (аутсорсинг) күшімен беріле ме жоқ па, оған тәуелсіз желілік қызмет көрсетуге қатысты барлық келісімдерге енгізілуге тиіс.
А.10.7 Ақпаратты тасымалдаушыларды басқару және оларды қорғау Мақсаты: Ақпараттық ресурстардың бүлінуін және ұйымның жұмысының кідіруін болдырмау.		
А.10.7.1	Ақпараттың түсіретін тасымалдаушыларын басқару	Басқару құралдары Ақпараттың түсіретін тасымалдаушыларын басқару рәсімдері орнатылуға тиіс.

A.10.7.2	Ақпаратты тасымалдаушыларды жою	Басқару құралдары Әрі қарай керек емес ақпаратты тасымалдаушылар заңды рәсімдерді сақтай отырып, қауіпсіз және сенімді әдіспен жойылуға тиіс.
A.10.7.3	Ақпаратпен айналысу рәсімдері	Басқару құралдары Ақпаратты санкцияланбаған ашудан немесе тиісті пайдаланбаудан қорғау үшін ақпаратпен айналысу рәсімдері және ақпаратты сақтау рәсімдері белгіленуге тиіс.
A.10.7.4	Жүйелік құжаттаманы қорғау	Басқару құралдары Жүйелік құжаттама санкцияланбаған қатынаудан қорғалған болуға тиіс.
A.10.8 Ақпаратпен алмасу Мақсаты: Ұйымның ішінде де, сонымен бірге кез келген сыртқы нысандармен де ақпараттық алмасу мәні болып табылатын ақпараттық және бағдарламалық қамтамасыз етудің қауіпсіздігін қамтамасыз ету.		
A.10.8.1	Ақпараттық алмасу саясаты және рәсімдері	Басқару құралдары Алмасудың заңды саясаты және рәсімдері, сондай-ақ алмасу құралдары барлық тұрпаттағы коммуникация құралдарын пайдалана отырып ақпараттың алмасуын қорғау үшін орнатылуға тиіс.
A.10.8.2	Алмасу туралы келісім	Басқару құралдары Ұйым мен шеттегі ұйымдар арасында ақпаратпен және бағдарламалық жабдықтаумен алмасу туралы келісімдер жасалуға тиіс.
A.10.8.3	Ақпаратты физикалық тасымалдаушыларды тасымалдау	Басқару құралдары Ұйымның аумағынан тыс тасымалдаған кезде ақпарат бар тасымалдағыштар санкцияланбаған қатынаудан бұрыс қолданудан немесе бүлінуден қорғалған болуға тиіс.
A.10.8.4	Электрондық хабар	Басқару құралдары Электрондық хабарлармен алмасу жүйелерінде таралатын ақпараттар тиісті жолмен қорғалуға тиіс.
A.10.8.5	Бизнестің ақпараттық жүйелері	Басқару құралдары Бизнестің ақпараттық жүйесін біріктірумен байланысты ақпаратты қорғау үшін рәсімдер және саясаттар әзірленуге және іске асырылуға тиіс.
A.10.9 Электрондық коммерция қызметі Мақсаты: Электрондық коммерция қызметінің қауіпсіздігін, сондай-ақ оларды қауіпсіз пайдалануды қамтамасыз ету.		
A.10.9.1	Электрондық коммерция	Басқару құралдары Электрондық коммерцияда пайдаланылатын және жалпыға ортақ желілер арқылы өтетін ақпарат, алаяқтық әрекеттерден, келісім-шарт бойынша даулардан, санкцияланбаған жарияланым және түрлендіруден қорғалған болуға тиіс.
A.10.9.2	Нақты уақыттағы операциялар (онлайн)	Басқару құралдары Онлайн операцияларында пайдаланылатын ақпарат толық берілмеуді болдырмау үшін, бұрыс маршруттау, санкцияланбаған хабарларды алмастыру, санкцияланбаған жариялау, санкцияланбаған көшіру немесе хабарды қайта жаңғырту қорғалған болуға тиіс.
A.10.9.3	Жалпыға ортақ ақпарат	Басқару құралдары Жалпыға ортақ жүйелерде айналымдағы ақпараттың тұтастығы санкцияланбаған түрлендіруді болдырмау үшін қорғалған болуға тиіс.

А.10.10 Мониторинг Мақсаты: Ақпаратты өңдеу бойынша санкцияланбаған әрекеттерді табу.		
А.10.10.1	Аудиттің журналын жүргізу	Басқару құралдары Пайдаланушылардың әрекеттерін тіркейтін аудиттің журналдары, ақпараттық қауіпсіздіктің ерекше жағдайлары және оқиғалары болашақтағы тексерулер және басқаруға қатынау мониторингіне көмектесу үшін белгіленген уақыт ішінде жүргізілуге және сақталуға тиіс.
А.10.10.2	Жүйені пайдалану мониторингі	Басқару құралдары Ақпаратты өңдеу құралдарын пайдаланудың мониторингі белгіленуге тиіс, ал мониторингтің нәтижелері жүйелі түрде талдануға тиіс.
А.10.10.3	Журналдар ақпаратын қорғау	Басқару құралдары Журналдарды жүргізу құралдары және ақпараттар журналы құпия әрекеттерден және санкцияланбаған қатынаудан қорғалған болуға тиіс.
А.10.10.4	Әкімгер және оператордың журналдары	Басқару құралдары Жүйелік әкімгер және жүйенің операторының әрекеті тиісті журналдарда тіркелуге тиіс.
А.10.10.5	Іркілістерді тіркеу	Басқару құралдары Іркілістер журналға тіркелуге, талдануға тиіс олар бойынша тиісті шаралар қолданылуға тиіс.
А.10.10.6	Жүйелік сағаттарды синхрондау	Басқару құралдары Ұйымның немесе қауіпсіздік доменінің шеңберіндегі ақпаратты өңдеудің барлық маңызды жүйелерінің сағаты нақты уақыттың белгіленген көзі бойынша синхрондалуға тиіс.
А.11 Қол жеткізуді басқару		
А.11.1 Қол жеткізуді басқаруға бизнес-талаптар Мақсаты: Ақпаратқа қол жеткізуді басқару.		
А.11.1.1	Қол жеткізуді басқару саясаты	Басқару құралдары Қол жеткізуді басқару саясаты белгіленуге, құжаттандырылуға және бизнес және қауіпсіздік тарапынан қол жеткізуге талаптарды ескере отырып қайта қаралуға тиіс.
А.11.2 Пайдаланушылардың қол жеткізуін басқару Мақсаты: Пайдаланушылардың санкцияланған қол жеткізуін қамтамасыз ету және ақпараттық жүйелерге санкцияланбаған қол жеткізуді болдырмау.		
А.11.2.1	Пайдаланушыларды тіркеу	Басқару құралдары Барлық ақпараттық жүйелерге және қызметтерге қол жеткізуді беру және жою үшін пайдаланушыларды тіркеудің заңды рәсімі және тіркеуді қабыл алмау рәсімі белгіленуге тиіс.
А.11.2.2	Өкілеттіктерді басқару	Басқару құралдары Өкілеттікті беру және пайдалану шектеулі және бақыланатын болуға тиіс.
А.11.2.3	Пайдаланушылардың парольдарын басқару	Басқару құралдары Парольдарды тағайындау басқарудың заңды процессі арқылы бақылануға тиіс.
А.11.2.4	Пайдаланушылардың қол жеткізу құқығын қайта қарау	Басқару құралдары Басшылар заңды процессті пайдалана отырып, жүйелі уақыт аралықтары арқылы пайдаланушылардың қол жеткізу құқығын қайта қарауға тиіс.

А.11.3 Пайдаланушылардың жауапкершілігі Мақсаты: Пайдаланушылардың санкцияланбаған қол жеткізуін, сондай-ақ ақпаратты және ақпаратты өңдеу құралдарын ұрлауды немесе компрометациялауды болдырмау.		
А11.3.1	Парольдарды пайдалану	Басқару құралдары Парольдарды таңдау және пайдалану кезінде пайдаланушылар өз тиімділігін практикада дәлелдеген қауіпсіздіктің қағидаларын ұстануға тиіс.
А.11.3.2	Қараусыз қалған пайдаланушының жабдығы	Басқару құралдары Пайдаланушылар қараусыз қалған жабдықтарды тиісті қорғаумен қамтамасыз етуге тиіс.
А.11.3.3	«Таза үстел» және «таза экран» саясаты	Басқару құралдары Ақпаратты түсіруші тасымалдаушылар және қағаздар үшін «таза үстел» саясаты және ақпаратты өңдеу құралдары үшін «таза экран» саясаты қабылдануға тиіс.
А.11.4 Желіге қол жеткізуді басқару Мақсаты: Желілік қызметтерге санкцияланбаған қол жеткізуді болдырмау.		
А.11.4.1	Желілік қызметтерді пайдалану саясаты	Басқару құралдары Пайдаланушылар пайдалану қызметтері оларға нақты рұқсат етілген қызметтерге ғана рұқсат алуға тиіс.
А.11.4.2	Сыртқы қосылу үшін пайдаланушыларды сәйкестендіру	Басқару құралдары Қашықтағы пайдаланушыларға қол жеткізуді бақылау үшін сәйкестендірудің тиісті әдістері қолданылуға тиіс.
А.11.4.3	Желідегі жабдықтарды сәйкестендіру	Басқару құралдары Жабдықтарды автоматты түрде сәйкестендіру нақты тораптармен және жабдықтармен орнатылатын қосылыстардың сәйкестендіру құралы ретінде қарастырылуға тиіс.
А.11.4.4	Қашықтағы диагностикалық және конфигурациялық портты қорғау	Басқару құралдары Диагностикалық және пішіндік порттарға физикалық және логикалық қатынау бақылануға тиіс.
А.11.4.5	Желілердегі бөліну	Басқару құралдары Желілерде ақпараттық қызметтер, пайдаланушылар және ақпараттық жүйелер топтары бөлінуге (оқшаулануға) тиіс.
А.11.4.6	Желілік қосылыстарды басқару	Басқару құралдары Ұжымдық пайдалану желілері үшін, әсіресе ұйымнан тысқары шығатындар үшін, пайдаланушылардың желіге қосылуға мүмкіндігі бизнес-қосымшаның (11.1-қараңыз) талаптарына және қол жеткізуді басқару саясатына сәйкес шектелуге тиіс.
А.11.4.7	Желілік маршруттауды басқару	Басқару құралдары Маршруттауды басқару құралдары компьютерлік жүйелерді қосу және ақпараттық ағындар бизнес-қосымшаға қол жеткізуді басқару саясатын бұзбайтынына кепілдік беретіндей болып іске асырылуға тиіс.
А.11.5 Операциялық жүйеге қол жеткізуді бақылау Мақсаты: Операциялық жүйелерге санкцияланбаған қол жеткізуді болдырмау.		
А.11.5.1	Кірудің қауіпсіздік рәсімдері	Басқару құралдары Операциялық жүйелерге қол жеткізу жүйеге қауіпсіз кіру рәсімімен бақылануға тиіс.

А.11.5.2	Пайдаланушыларды сәйкестендіру және сәйкестендіру	Басқару құралдары Барлық пайдаланушылардың тек жеке пайдалану үшін ғана бірегей сәйкестендіргіші (пайдаланушының ИД) болуға тиіс, сондай-ақ пайдаланушының мәлімденген жеке басын растау үшін лайықты сәйкестендіру әдісі таңдап алынуға тиіс.
А.11.5.3	Парольдарды басқару жүйесі	Басқару құралдары Парольдарды басқару жүйелері интерактивті болуға тиіс және сапалы парольмен қамтамасыз етуге тиіс.
А.11.5.4	Жүйелік утилиттерді пайдалану	Басқару құралдары Олардың көмегімен жүйені және қосымшаларды басқару құралдарын өзгертуге болатын жүйелік утилит-бағдарламаларды пайдалану шектеулі болуға және қатаң бақылануға тиіс.
А.11.5.5	Уақыт бойынша сеансты блоктау	Басқару құралдары Белсенді емес әрекет етпейтін сеанстар берілген уақыттың ішінде жабылуға тиіс.
А.11.5.6	Қосылу уақыты бойынша шектеулер	Басқару құралдары Қосылу уақыты бойынша шектеулер жоғары тәуекелден қосымшаларды қосымша қорғаумен қамтамасыз ету үшін пайдаланылуға тиіс
А.11.6 Қосымшаларға және олардың ақпаратына қол жеткізуді басқару Мақсаты: Ақпараттық жүйелерде сақталатын ақпараттарға санкцияланбаған қол жеткізуді болдырмау.		
А.11.6.1	Ақпаратқа қол жеткізуді шектеу	Басқару құралдары Пайдаланушылар мен қызмет көрсетуші қызметкерлердің ақпаратқа және қолданбалы жүйелердегі қызметтерге қол жеткізуі қол жеткізуді басқарудың берілген саясатына сәйкес шектелуге тиіс.
А.11.6.2	Қиын жүйелерді оқшаулау	Басқару құралдары Қиын жүйелер бөлінген (оқшауланған) есептеуіш ортада қызмет істеуге тиіс.
А.11.7 Жедел есептеу және қашықтықтағы жұмыс (teleworking) Мақсаты: Қашықтықтағы жұмыс және жедел есептеу құралдарын пайдаланған кезде ақпараттық қауіпсіздікті қамтамасыз ету.		
А.11.7.1	Жедел есептеу және коммуникациялар	Басқару құралдары Жедел есептеу және коммуникация құралдарын пайдаланумен байланысты тәуекелдерден қорғауды қамтамасыз ету үшін заңды саясат болуға тиіс және тиісті қауіпсіздік шаралары қабылдануға тиіс.
А.11.7.2	Қашықтықтағы жұмыс	Басқару құралдары Қашықтықтағы жұмыс үшін саясат, жедел жоспарлар мен рәсімдер әзірленіп, іске асырылуға тиіс.
А.12 Ақпараттық жүйелерді алу, әзірлеу және алып жүру		
А.12.1 Ақпараттық жүйелердің қауіпсіздігіне қойылатын талаптар Мақсаты: Қауіпсіздік ақпараттық жүйелердің компоненті болып табылатындығына кепілдік беру.		
А.12.1.1	Қауіпсіздікке қойылатын талаптарды талдау және егжей-тегжейін ашу	Басқару құралдары Жаңа ақпараттық жүйелерге немесе қолданыстағы ақпараттық жүйелердің түрленімдеріне бизнес-талаптарды тұжырымдау қауіпсіздікті басқару құралдарына талаптарды белгілеуге тиіс.

А.12.2 Қосымшалардағы сыпайы өңдеулер Мақсаты: Қосымшалардағы ақпараттың қателерін, жоғалуын, санкцияланбаған түрлендіруін немесе тиісті түрде пайдаланылмауын болдырмау.		
А.12.2.1	Кіріс деректерінің дұрыстығын тексеру	Басқару құралдары Осы деректер түзетілген және дұрыс болып табылатындығына кепілдік беру үшін қосымшалардың кіріс деректеріне тексеру жүргізілуге тиіс.
А.12.2.2	Ішкі өңдеуді бақылау	Басқару құралдары Дұрыстықты тексеру өңдеу кезіндегі қателерден немесе әдейілеп істелген әрекеттерден ақпараттың кез келген бүлінуін анықтау үшін қосымшаларға салынуға тиіс.
А.12.2.3	Хабардың тұтастығы	Басқару құралдары Қосымшалардағы хабарлардың тұтастығын қорғау және түпнұсқалығына кепілдік беру талаптары сәйкестендірілуге тиіс және басқарудың тиісті құралдары сәйкестендірілуге және іске асырылуға тиіс.
А.12.2.4	Шығыс деректерінің дұрыстығын тексеру	Басқару құралдары Сақталатын ақпаратты өңдеу дұрыс және ағымдағы жағдайларға сәйкес келетіндігіне кепілдік беру үшін дұрыстығы тексерілуге тиіс.
А.12.3 Криптографиялық басқару құралдары Мақсаты Криптографиялық құралдармен ақпараттың құпиялығын, түпнұсқалығын және тұтастығын қорғауды қамтамасыз ету.		
А.12.3.1	Криптографиялық басқару құралдарын пайдалану саясаты	Басқару құралдары Ақпаратты қорғау үшін криптографиялық басқару құралдары әзірленуге және іске асырылуға тиіс.
А.12.3.2	Кілттерді басқару	Басқару құралдары Кілттерді басқару ұйымда криптографиялық әдістердің қолданылуын қолдау үшін іске асырылуға тиіс.
А.12.4 Жүйелік файлдардың қауіпсіздігі Мақсаты: Жүйелік файлдардың қауіпсіздігін қамтамасыз ету.		
А.12.4.1	Өндірістік бағдарламалық жабдықтауды бақылау	Басқару құралдары Өндірістік жүйелерде бағдарламалық жабдықтауды орнатуға бақылау рәсімдері болуға тиіс.
А.12.4.2	Жүйелік сынақтама деректерін қорғау	Басқару құралдары Сынақтау деректері мұқият таңдап алынуға тиіс, сондай-ақ қорғалған және бақыланатын болуға тиіс.
А.12.4.3	Бағдарламаның бастапқы кодына қол жеткізуді басқару	Басқару құралдары Бағдарламалардың бастапқы кодына қол жеткізу шектелуге тиіс.
А.12.5 Әзірлеу процесстерінің және техникалық қызмет көрсету қауіпсіздігі Мақсаты: Бағдарламалық жабдықтау және қолданбалы жүйелердің ақпаратының қауіпсіздігін қолдау.		
А.12.5.1	Өзгертулерді басқару рәсімдері	Басқару құралдары Өзгертулерді іске асыру өзгертулерді басқарудың заңды рәсімдерінің көмегімен бақылануға тиіс.
А.12.5.2	Өндірістік жүйені өзгерткеннен кейін қосымшаға техникалық талдау жасау	Басқару құралдары Бизнес-қосымша үшін қиын өндірістік жүйелерді өзгерткен кезде ұйымның қауіпсіздігіне және қызмет істеуіне қолайсыз әрекет етуінің жоқтығына кепілдік беру үшін талданудан өткізілуге және сынақтан өткізілуге тиіс.

А.12.5.3	Бағдарламалық жабдықтау пакеттерін өзгертуді шектеу	Басқару құралдары Бағдарламалық жабдықтау пакеттерін түрлендіру сөзсіз мақұлдануға тиіс, түрлендіру тек қажетті өзгертулермен ғана шектелуге тиіс және барлық өзгертулер қатаң бақылануға тиіс.
А.12.5.4	Ақпараттың жойылуы	Басқару құралдары Ақпараттың жойылуына мүмкіндіктерді болдырмауға тиіс.
А.12.5.5	Аутсорсинг жағдайында бағдарламалық жабдықтауды әзірлеу	Басқару құралдары Шеттегі ұйымдармен (аутсорсинг) бағдарламалық жабдықтауды әзірлеу ұйыммен бақылануға және қадағалануға тиіс.
А.12.6 Техникалық осалдықтарды басқару Мақсаты: Техникалық осалдықтар туралы жарияланған деректерден туындайтын тәуекелдерді азайту.		
А.12.6.1	Техникалық осалдықты басқару	Басқару құралдары Ақпараттық жүйелердің техникалық осалдығы туралы ақпаратты дер кезінде алу керек, осы осалдықтардан ұйымның қорғалмауы бағалануға тиіс және осындай осалдықпен байланысты тәуекелдерді жою үшін барабар шаралар қолданылуға тиіс.
А.13 Ақпараттық қауіпсіздіктің оқыс оқиғаларын басқару		
А.13.1 Ақпараттық қауіпсіздік оқиғалары және қорғаныстың осалдығы жөнінде есеп жасау Мақсаты Ақпараттық жүйелермен байланысты ақпараттық қауіпсіздік оқиғалары және қорғаныс осалдықтары туралы кепілдік беру, бұл дер кезінде түзетуші шаралар қабылдауға жағдай жасайтындай жолмен хабарланады.		
А.13.1.1	Ақпараттық қауіпсіздік оқиғалары туралы хабар	Басқару құралдары Ақпараттық қауіпсіздік оқиғалары туралы мүмкіндігінше тезірек тиісті басқарушы арналар бойынша хабарлануға тиіс.
А.13.1.2	Қорғаныстың осалдығы туралы хабар	Басқару құралдары Ақпараттық жүйелер мен қызметтерді пайдаланатын шеттегі ұйымдардың барлық қызметкерлерін, мердігерлерін және пайдаланушыларын жүйелер немесе қызметтердің барлық бақыланатын немесе болжанған осалдығын белгілеуге және хабарлауға міндеттеу керек.
А.13.2 Ақпараттық қауіпсіздікті жетілдіру және оқыс оқиғаларын басқару Мақсаты: Ақпараттық қауіпсіздіктің оқыс оқиғаларын басқаруға тиімді және қарама-қайшы келмейтін жолды қолдануға кепілдік беру.		
А.13.2.1	Жауапкершілік және рәсімдер	Басқару құралдары Ақпараттық қауіпсіздіктің оқыс оқиғаларына тез, тиімді және дұрыс әрекет етуді қамтамасыз ету үшін рәсімдер және басшылардың жауапкершілігі белгіленуге тиіс.
А.13.2.2	Ақпараттық қауіпсіздіктің оқыс оқиғаларына оқыту	Басқару құралдары Ақпараттық қауіпсіздіктің оқыс оқиғаларының тұрпаттарын, көлемдерін және құнын өлшеу және қадағалауға жағдай жасайтын механизмдер іске асырылуға тиіс.
А.13.2.3	Дәлелдемелер жинау	Басқару құралдары Егер ақпараттық қауіпсіздіктің оқыс оқиғаларының нәтижесіндегі әрекеттерді өзіне құқықтық әрекеттер кіретін (азаматтық, сондай-ақ қылмыстық кодекс бойынша да) ұйымға немесе тұлғаға қатысты қолдану болжанатын болса, тиісті құқық қорғау органында (органдарында) белгіленген дәлелдеме ережелерін орындау үшін дәлелдеме жиналуға, сақталуға және ұсынылуға тиіс.

А.14 Бизнестің үздіксіздігін басқару		
А.14.1 Бизнестің үздіксіздігін басқарудағы ақпараттық қауіпсіздік аспектілері Мақсаты: Бизнес-қызметтердегі іркілістерге қарсы тұру және қиын жағдайдағы бизнес-процестерді ақпараттық жүйелердің ірі апаттарынан немесе қирауларының салдарынан қорғауды қамтамасыз ету.		
А.14.1.1	Бизнестің үздіксіздігін басқару процессіне ақпараттық қауіпсіздікті енгізу	Басқару құралдары Осы ұйымның бизнесінің үздіксіздігі үшін қажетті ақпараттық қауіпсіздіктің талаптары ескеретін ұйымның шеңберіндегі бизнестің үздіксіздігін қамтамасыз етудің басқарылатын процессі әзірленуге және қолдау алуға тиіс.
А.14.1.2	Бизнестің үздіксіздігі және тәуекелдерді бағалау	Басқару құралдары Бизнес-процестердің тоқтап қалу мүмкіндігі бар оқиғалар сәйкестендірілуге тиіс, сондай-ақ осындай тоқтап қалулардың әрекеті және ықтималдығы және олардың ақпараттық қауіпсіздікке әсері айқындалуға тиіс.
А.14.1.3	Ақпараттық қауіпсіздік кіретін үздіксіздікті қамтамасыз ететін жоспарларды әзірлеу және іске асыру	Басқару құралдары Қиын жағдайдағы бизнес-процесстер тоқтағаннан немесе іркілісінен кейін талап етілген деңгейде және талап етілген уақытта ақпаратқа қол жеткізуге кепілдік беретін операцияларды қалпына келтіру және қамтамасыз ету бойынша жоспарлар әзірленуге және іске асырылуға тиіс.
А.14.1.4	Бизнестің үздіксіздігін жоспарлау құрылымы	Басқару құралдары Сынақтау және алып жүру үшін артықшылықтарды анықтау және ақпараттық қауіпсіздік талаптарын үздіксіз есепке алу, барлық жоспарлардың қарама-қайшы еместігін қамтамасыз етуге кепілдік беру үшін бизнестің үздіксіздігін қамтамасыз ету жоспарының бірегей құрылымы ұсталуға тиіс.
А.14.1.5	Бизнестің үздіксіздігін қамтамасыз ету жоспарларын сынақтау, алып бару және қайта бағалау	Басқару құралдары Бизнестің үздіксіздігін қамтамасыз ету жоспарлары олардың маңыздылығына және тиімділігіне кепілдік беру үшін жүйелі түрде жаңартылуға және сыналуға тиіс.
А.15 Заңды талаптарға сәйкестігі		
А.15.1 Құқықтық талаптарға сәйкестігі Мақсаты: Міндеттемелер, реттеуші немесе шарттық міндеттемелер, сондай-ақ қауіпсіздіктің барлық талаптар заңына негізделген заңдарды бұзудан аулақ болу.		
А.15.1.1	Қажетті құқықтық базаны айқындау	Басқару құралдары Әрбір ақпараттық жүйелер және ұйымдар үшін заңның барлық талаптары, реттеуші және шарттық талаптар, сондай-ақ осы талаптарды қанағаттандыру үшін пайдаланылатын ұйымның әдістері маңызды жағдайда қолдау алуға және нақты айқындалуға, құжаттандырылуға тиіс.
А.15.1.2	Санаткерлік меншікке құқық (IPR)	Басқару құралдары Санаткерлік меншіктік, сондай-ақ патенттелген бағдарламалық өнімдерді пайдалану бойынша құқық таралатын материалдарды пайдалану бойынша құқықтық, реттеуші және шарттық талаптарға сәйкестікке кепілдік беретін тиісті рәсімдер іске асырылуға тиіс.
А.15.1.3	Ұйымның жазбаларын қорғау	Басқару құралдары Маңызды жазбалар заңның талаптарына, реттеуші және шарттық талаптарға, сондай-ақ бизнес талаптарға сәйкес жоғалудан, жойылудан және жалған жасалудан қорғалуға тиіс.

А.15.1.4	Жеке ақпараттардың деректерін және құпиялығын қорғау	Басқару құралдары Деректерді және құпиялықты қорғау, егер шарттардың ережелері қолданылатын болса, тиісті заңнама, реттеуші ережелерге сәйкес қамтамасыз етілуге тиіс.
А.15.1.5	Ақпаратты өңдеу құралдарын тиісті пайдаланбауды болдырмау	Басқару құралдары Пайдаланушылар санкцияланбаған мақсаттар үшін ақпаратты өңдеу құралдарын пайдаланбауға тиіс.
А.15.1.6	Криптографиялық басқару құралдарын реттеу	Басқару құралдары Криптографиялық басқару құралдары барлық тиісті келісімдерге, заңдарға және реттеуші ережелерге сәйкес пайдаланылуға тиіс.
А.15.2 Қауіпсіздік саясатына және стандарттарға сәйкестік, техникалық сәйкестік Мақсаты: Қауіпсіздіктің саясаты және стандарттарымен қабылданған жүйелерге сәйкестікті қамтамасыз ету.		
А.15.2.1	Қауіпсіздіктің саясаттары мен стандарттарына сәйкестік	Басқару құралдары Менеджерлер қауіпсіздіктің саясаты және стандарттарына сәйкестікті қамтамасыз ететініне, барлық қауіпсіздік рәсімдері және олардың жауапкершілік салалары дұрыс орындалатындығына кепілдік беруге тиіс.
А.15.2.2	Техникалық сәйкестікті тексеру	Басқару құралдары Ақпараттық жүйелер қауіпсіздікті қамтамасыз ету стандарттарына сәйкестікке жүйелі түрде тексерілуге тиіс.
А.15.3 Ақпараттық жүйелер аудитін талдау Мақсаты: Ақпараттық жүйелердегі аудит процессінде бір жағынан, аудит процессінің тиімділігін арттыру және екінші жағынан ақпараттық жүйелерге аудит процессінің әсер етуін азайту.		
А.15.3.1	Ақпараттық жүйелердің аудитін басқару құралдары	Басқару құралдары Өндірістік жүйелерді тексеру кіретін аудит және қызметтің талаптары, бизнес-процесстерде іркілістер тәуекелін азайту үшін мұқият жоспарлануға және келісілуге тиіс.
А.15.3.2	Ақпараттық жүйелер аудитінің құралдарын қорғау	Басқару құралдары Ақпараттық жүйелер аудитінің құралдарына қол жеткізу кез келген тиісті пайдаланбау мүмкіндігін немесе компрометацияны болдырмау үшін қорғалған болуға тиіс.

Б қосымшасы
(анықтамалық)
OECD қағидаттары және осы стандарт

OECD Guidelines for the Security of Information Systems and Networks [1] құжатында келтірілген қағидалар ақпараттық жүйелер мен желілердің қауіпсіздігі басқарылатын барлық саясаттарға және қызмет істеудің барлық деңгейлеріне қолданылады. Осы стандарт В.1-кестеде көрсетілгендей **4**, **5**, **6**, **7** және **8**-тармақтарында сипатталғандай ПРОК үлгісі және процесстері көмегімен OECD кейбір қағидаларын іске асыру үшін ақпараттық қауіпсіздікті басқару жүйесінің жалпы сұлбасын білдіреді.

Б.1-кесте –OECD қағидалары және ПРОК үлгісі

OECD қағидасы	**АҚБЖ тиісті процессі және ПРОК сатысы**
Мәліметтілік (Awareness) Процесске қатысушылар ақпараттық жүйелер мен желілерді қорғау қажеттігі туралы, сондай-ақ қауіпсіздікті арттыру үшін олар не істей алатындығы туралы хабардар етілуге тиіс.	Бұл қызмет **Іске асыру** сатысының (**4.2.2** және **5.2.2 қараңыз**) құрамды бөлігі болып табылады.
Жауапкершілік Процесске қатысушылардың барлығы ақпараттық жүйелер мен желілердің қауіпсіздігі үшін жауапкершілік көтереді.	Бұл қызмет **Іске асыру** сатысының (**4.2.2** және **5.1 қараңыз**) құрамды бөлігі болып табылады.
Әрекет ету Процесске қатысушылар қауіпсіздіктің оқыс оқиғасын табу және болдырмау, сондай-ақ оларға әрекет ету үшін дер кезінде және келіскен түрде әрекет етуге тиіс.	Ішінара **Тексеру сатысында** (**4.2.3** және **6–7.3 қараңыз**) мониторингке және **Жетілдіру** (**4.2.4** және **8.1–8.3 қараңыз**) сатысында әрекет етуге сәйкес келеді. Одан басқа, **Жоспарлау** және **Тексеру** сатыларының кейбір аспектілерімен қамтылуы мүмкін.
Тәуекелдерді бағалау Процесске қатысушылар тәуекелдерді бағалауды орындауға тиіс.	Бұл қызмет **Жоспарлау** (**4.2.1 қараңыз)** сатысының құрамды бөлігі болып табылады, ал тәуекелдерді қайта бағалау **Тексеру** (**4.2.3** және **6–7.3 қараңыз**) сатысының бөлігі болып табылады.
Қауіпсіздікті әзірлеу және іске асыру Процесске қатысушылар ақпараттық жүйелер мен желілердің маңызды элементтерінің қатарына қауіпсіздікті енгізуге тиіс.	Тәуекелдерді бағалау аяқталуы бойынша тәуекелдерді өңдеу үшін басқару құралдары таңдап алынады, да **Жоспарлау** (**4.2.1 қараңыз**) сатысының құрамды бөлігі болып табылады. Содан кейін **Іске асыру** (**4.2.2** және **5.2 қараңыз**) сатысы осы басқару құралдарын жұмысқа пайдалану және іске асырылуын қамтиды.
Қауіпсіздікті басқару Процесске қатысушылар қауіпсіздікті басқаруға кешенді жол қабылдауға тиіс.	Тәуекелдерді басқару– бұл өзіне оқыс оқиғаларды болдырмауды, анықтауды және әрекет етуді кіргізетін процесс, үздіксіз алып жүру, анализ және аудит. Барлық осы аспектілер **Жоспарлау, Іске асыру, Тексеру** және **Жетілдіру** сатыларымен қамтылады.
Қайта бағалау Процесске қатысушылар ақпараттық жүйелер мен желілер қауіпсіздігін қайта қарауға және қайта бағалауға тиіс, сондай-ақ қауіпсіздіктің саясатына, критерийлеріне және рәсімдеріне қажетті өзгертулер енгізуге тиіс.	Ақпараттық қауіпсіздікті қайта бағалау **Тексеру** (**4.2.3** және **6–7.3 қараңыз**) сатысының құрамды бөлігі болып табылады, онда ақпараттық қауіпсіздікті басқару жүйесінің тиімділігін тексеру үшін жүйелі түрде талдау жүргізіледі; қауіпсіздікті арттыру **Жетілдіру** (**4.2.4** және **8.1–8.3 қараңыз**) сатысының құрамды бөлігі болып табылады.

В қосымша
(анықтамалық)
ҚР СТ ИСО 9001-2001, ҚР СТ ГОСТ Р ИСО 14001:2000 стандарттары және осы стандарттар арасындағы сәйкестік

В.1-кестесінде *ҚР СТ ИСО* 9001-2001, ҚР СТ ГОСТ Р ИСО 14001:2000 стандарттары мен осы стандарт арасындағы сәйкестік берілген.

В.1-кестесі— *ҚР СТ ИСО* 9001-2001, ҚР СТ ГОСТ Р ИСО 14001:2000 стандарттары мен осы стандарт арасындағы сәйкестік

Осы стандарт	**ҚР СТ ИСО 9001:2001**	**ҚР СТ ГОСТ Р ИСО 14001:2000**
Кіріспе	**Кіріспе**	**Кіріспе**
Жалпы ережелер	Жалпы ережелер	
Процестік тәсіл	Процестік тәсіл	
	ISO 9004 стандартымен байланыс	
Басқа басқару жүйелерімен үйлесімділігі	Басқа басқару жүйелерімен үйлесімділігі	
1 Пайдалану саласы	**1 Пайдалану саласы**	**1 Пайдалану саласы**
1.1 Жалпы ережелер	1.1 Жалпы ережелер	
1.2 Қолданушылығы	1.2 Қолданушылығы	
2 Нормативтік сілтемелер	**2 Нормативтік сілтемелер**	**2 Нормативтік сілтемелер**
3 Терминдер мен анықтамалар	**3 Терминдер мен анықтамалар**	**3 Терминдер мен анықтамалар**
4 Ақпараттық қауіпсіздікті басқару жүйесі	**4 Сапа менеджменті жүйесі**	**4 Қоршаған ортаны басқару жүйесіне талаптар**
4.1 Жалпы ережелер	4.1 Жалпы ережелер	4.1 Жалпы ережелер
4.2 АҚБЖ әзірлеу және басқару		
4.2.1 АҚБЖ әзірлеу		
4.2.2 АҚБЖ іске асыру және пайдалану		4.4 Іске асыру және пайдалану
4.2.3 АҚБЖ мониторингі және талдау	8.2.3 Мониторинг және процесстерді өлшеу	4.5.1 Мониторинг және өлшеу
	8.2.4 Мониторинг және өнімнің процесстерін өлшеу	
4.2.4 АҚБЖ алып жүру және жетілдіру		
4.3 Құжаттамаларға талаптар	4.2 Құжаттамаларға талаптар	
4.3.1 Жалпы талаптар	4.2.1 Жалпы талаптар	
	4.2.2 Сапа жөніндегі нұсқау	
4.3.2 Құжаттарды басқару	4.2.3 Құжаттарды басқару	4.4.5 Құжаттамаларды басқару
4.3.3 Жазбаларды басқару	4.2.4 Жазбаларды басқару	4.5.4 Жазбаларды басқару

5 Қызметкерлердің міндеттерін үлестіру 5.1 Басшылықтың жолын ұстаушы	**5 Қызметкерлердің міндеттерін үлестіру** 5.1 Өкілеттіктерді табыстау 5.2 Тұтынушыға жинақталу 5.3 Сапа саясаты 5.4 Жоспарлау 5.5 Жауапкершілік, өкілеттілік және коммуникация	 4.2 Қызмет етудің орта саясаты 4.3 Жоспарлау
5.2 Ресурстарды басқару 5.2.1 Ресурстарды беру 5.2.2 Оқыту, мәліметтілік және біліктілік	**6 Ресурстарды басқару** 6.1 Ресурстарды беру 6.2 Адам ресурстары 6.2.2 Біліктілік, мәліметтілік және оқыту 6.3 Инфрақұрылым 6.4 Жұмыс ортасы	 4.2.2 Біліктілік, оқыту және мәліметтілік
6 АҚБЖ ішкі аудиттары	8.2.2 Ішкі аудиттар	4.5.5 Ішкі аудиттар
7 Басшылықтың АҚБЖ қайта қарауы 7.1 Жалпы ережелер 7.2 Талдау үшін бастапқы деректер 7.3 Талдау қорытындылары	**5.6 Кейбір ережелерді қайта қарау рәсімін басқару** 5.6.1 Жалпы ережелер 5.6.2 Талдау үшін бастапқы деректер 5.6.3 Талдау қорытындылары	**4.6 Кейбір ережелерді қайта қарау рәсімін басқару**
8 АҚБЖ жетілдіру 8.1 Үздіксіз жетілдіру 8.2 Түзетушілік әсер ету 8.3 Ескертпешілік әсер ету	**8.5 Жетілдіру** 8.5.1 Үздіксіз жетілдіру 8.5.3 Түзетушілік әсер ету 8.5.3 Ескертпешілік әсер ету	 4.5.3 Сәйкес келмейтін және түзетушілік әсер ету, ескертпешілік әсер ету
А қосымшасы. Басқару мақсаттары және басқару құралдары **Б қосымшасы. OECD қағидалары және осы стандарт** **В қосымшасы. ҚР СТ ИСО 9001:2001, ISO 14001:2004 стандарттары және осы стандарт арасындағы сәйкестік**	**А қосымшасы. ҚР СТ ИСО 9001:2001, ҚР СТ ГОСТ Р ИСО 14001:2000 стандарттар арасындағы сәйкестік**	**А қосымшасы. Осы стандартты пайдалану жөніндегі нұсқау** **Б қосымшасы. ISO 14001:2004 және ISO 9001:2000 арасындағы сәйкестік**

Қосымша
(анықтамалық)

Библиография

Стандарттар жарияланымы

[1] ҚР СТ ИСО 9001:2001, Сапа менеджменті жүйесі. Талаптар

[2] ISO/IEC 13335-1:2004, Information technology— Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

[3] ISO/IEC TR 13335-3:1998, Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security

[4] ISO/IEC TR 13335-4:2000, Information technology— Guidelines for the management of IT Security — Part 4: Selection of safeguards

[5] ҚР СТ ГОСТ Р ИСО 14001-2000 Қоршаған ортаны басқару жүйелері. Қолдану жөніндегі талаптар және нұсқаулар

[6] ISO 14001:2004, Environmental management systems — Requirements with guidance for use

[7] ISO/IEC TR 18044:2004, Information technology— Security techniques — Information security incident management

[8] ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing

[9] ISO/IEC Guide 62:1996, General requirements for bodies operating assessment and certification/registration of quality systems

[10] ISO/IEC Guide 73:2002, Risk management— Vocabulary— Guidelines for use in standards

Басқа жарияланымдар

[1] OECD, Guidelines for the Security of Information Systems and Networks— Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

[2] NIST SP 800-30, Risk Management Guide for Information Technology Systems

[3] Deming W.E., Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986

„

ӘОЖ 681.324:006.354 **МСЖ 13.060**

Түйінді сөздер: ақпараттық қауіпсіздік, ақпараттық қауіпсіздікті басқару жүйесі, АҚБЖ, тәуекелді бағалау, тәуекелді өңдеу, ақпараттық қауіпсіздік саясаты, басқару мақсаттары, басқару құралдары.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Требования

СТ РК ИСО/МЭК 27001-2008

(ИСО/МЭК 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования», IDT)

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 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования» («Information technology. Security techniques. Information security management systems. Requirements), IDT, с дополнительными требованиями, отражающими потребности экономики Республики Казахстан, которые выделены курсивом.

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2013 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

Настоящий стандарт подготовлен для использования в качестве модели для разработки, реализации, эксплуатации, мониторинга, анализа, сопровождения и модернизации системы управления информационной безопасностью (СУИБ). Принятие СУИБ должно являться для организации стратегическим решением. На архитектуру и реализацию СУИБ организации влияют цели и потребности бизнеса, требования к безопасности, используемые процедуры, а также размер и структура самой организации. Предполагается, что со временем перечисленные характеристики и поддерживающие их системы изменяются. Предполагается, что реализация СУИБ будет масштабироваться в соответствии с потребностями организации.

Настоящий стандарт может использоваться для оценки соответствия заинтересованными внутренними и внешними сторонами.

В настоящем стандарте принят процессный подход к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ организации.

Чтобы функционировать эффективно, организация должна идентифицировать и управлять различными действиями. Любое действие, использующее ресурсы и управляемое с целью преобразования входных данных в выходные, может рассматриваться как процесс. Часто выходные данные одного процесса непосредственно представляют входные данные для следующего процесса.

Применение системы процессов в организации, вместе с идентификацией и взаимодействием этих процессов, а также управлением этими процессами может быть названо «процессным подходом».

Процессный подход к управлению информационной безопасностью, представленный в настоящем стандарте, побуждает своих пользователей придавать особое значение следующему:

а) пониманию требований информационной безопасности организации и необходимости определить политику и цели информационной безопасности;

б) внедрению и использованию средств управления для управления рисками информационной безопасности организации в контексте общих бизнес-рисков организации;

в) мониторингу и анализу производительности и эффективности СУИБ;

г) постоянному совершенствованию, основанному на объективных показателях.

В настоящем стандарте принята модель «Планирование – Реализация – Оценка – Корректировка - ПРОК» («Plan – Do – Check - Act» – PDCA), которая применена для структурирования всех процессов СУИБ. На рисунке 1

показано, как СУИБ принимает в качестве входных данных требования к информационной безопасности и ожидания заинтересованных сторон и в результате ряда необходимых действий и процессов дает на выходе информационную безопасность, которая удовлетворяет этим требованиям и ожиданиям. Кроме того, на рисунке 1 показаны связи в процессах, представленных в пунктах 4, 5, 6, 7 и 8.

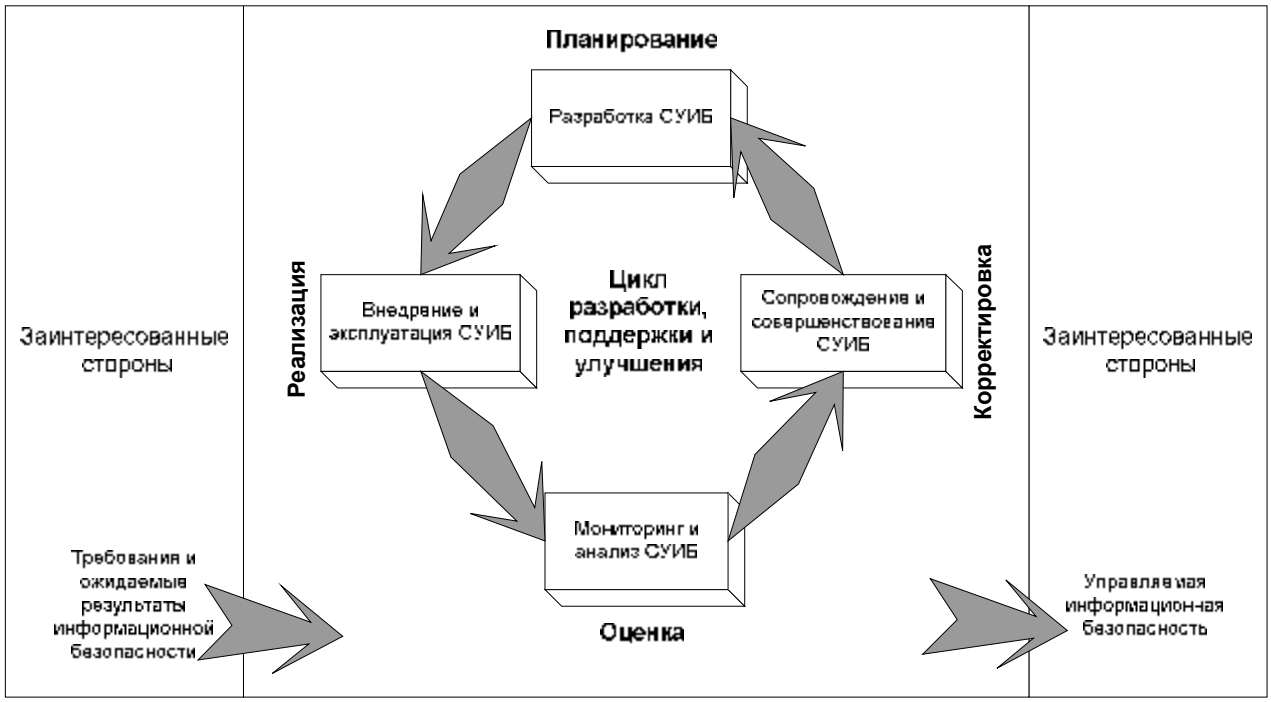


Рисунок 1. Модель ПРОК в применении к процессам СУИБ

Принятие модели ПРОК также отражает принципы, изложенные в документе OECD Guidelines (2002)[1] - руководящем документе по безопасности информационных систем и сетей. Настоящий стандарт предлагает устойчивую модель для реализации изложенных в упомянутом документе принципов, регулирующих оценку рисков, планирование и реализацию безопасности, управление безопасностью и переоценку.

Пример 1. Одним из требований может быть следующее: нарушения информационной безопасности не должны причинять серьезного финансового ущерба организации и/или создавать затруднения в деятельности организации.

Пример 2. Одним из ожиданий может быть следующее: в случае серьезного инцидента (например, успешной атаки на web-сайт организации, используемый для электронного бизнеса) сотрудники будут иметь достаточную подготовку в использовании соответствующих процедур, чтобы минимизировать воздействие.

[1] OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

Планирование (разработка СУИБ)	Определение политики СУИБ, целей, процессов и процедур, значимых для управления рисками и повышения информационной безопасности, с целью получения результатов, соответствующих общим политикам и целям организации.
Реализация (внедрение и эксплуатация СУИБ)	Реализация и использование политики СУИБ, средств управления, процессов и процедур.
Проверка (мониторинг и анализ СУИБ)	Оценка и, если требуется, измерение характеристик процесса для проверки соответствия политике СУИБ, целям и практическому опыту, а также передача результатов для последующего анализа управленческим персоналом.
Совершенствование (сопровождение и совершенствование СУИБ)	Принятие корректирующих и превентивных мер по результатам внутреннего аудита СУИБ и анализа, выполненного управленческим персоналом, а также на основе другой значимой информации, с целью постоянного совершенствования СУИБ.

Настоящий стандарт согласован со стандартами *СТ РК 9001-2001* и ISO 14001:2004, чтобы обеспечить исполнение и применение, совместимые и интегрированные с родственными стандартами управления. Таким образом, одна надлежащим образом разработанная система управления может удовлетворять требованиям всех этих стандартов. Таблица В.1 (Приложение В) иллюстрирует взаимосвязи между пунктами настоящего стандарта, стандарта *СТ РК ИСО 9001-2001 Система менеджмента качества. Требования* и международного стандарта ISO 14001:2004 (Действующий стандарт: *СТ РК ИСО 14001-2000 Системы управления окружающей средой. Требования и руководство по применению*).

Настоящий стандарт разработан так, чтобы организация могла выстроить или интегрировать свою СУИБ в соответствии с родственными требованиями к системам управления.

ВАЖНО! Настоящий стандарт не подразумевает, что в него включено все необходимое для обеспечения информационной безопасности. Пользователи несут ответственность за правильное применение стандарта. Само по себе соответствие стандарту не освобождает от правовых обязательств.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
Требования

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт применим для всех типов организаций (например, коммерческих предприятий, правительственных учреждений, некоммерческих организаций). Настоящий стандарт определяет требования к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию документированной **системой управления информационной безопасностью (далее –** СУИБ) в контексте общих бизнес-рисков организации. Он определяет требования к реализации средств управления, соответствующих потребностям отдельных организаций или их частей.

СУИБ разрабатывается для обеспечения адекватных и соразмерных средств управления безопасностью, которые защищают информационные ресурсы и обеспечивают конфиденциальность для заинтересованных сторон.

Примечание 1. В настоящем стандарте термин «бизнес» следует понимать в широком смысле, этим термином обозначается любая деятельность, которая необходима для достижения целей, ради которых существует организация.

Примечание 2. В стандарте ИСО/МЭК 17799 приводится руководство по применению, которым можно воспользоваться при разработке средств управления.

Требования, определенные в настоящем стандарте, являются общими и предназначены для использования во всех организациях, независимо от их типа, величины и вида деятельности. Исключение любого из требований, приведенных в пунктах 4, 5, 6, 7 и 8, не допускается, если организация объявляет о соответствии настоящему стандарту.

Все исключения средств управления, признанные необходимыми для соответствия критериям принятия рисков, должны быть обоснованы, и должны быть предоставлены доказательства, что соответствующие решения о принятии рисков были приняты ответственными лицами. Если исключаются какие-либо средства управления, заявления о соответствии настоящему стандарту недопустимы, кроме тех случаев, когда исключения не влияют на способность и/или обязательства организации обеспечивать информационную безопасность, которая удовлетворяет требованиям к безопасности, определенным по результатам оценки рисков, и соответствующим требованиям закона и нормативных документов.

Примечание. Если организация уже имеет действующую систему управления бизнес-процессами (например, соответствующую стандарту *СТ РК ИСО 9001* или *СТ РК ИСО 14001*), то в большинстве случаев предпочтительнее удовлетворить требования настоящего стандарта в рамках этой существующей системы управления.

2 Нормативные ссылки

Следующие нормативно-справочные документы обязательны для применения настоящего стандарта. Если указана дата документа, то следует использовать только указанную редакцию документа. Если дата документа не указана, используется последняя редакция указанного документа (включающая все поправки).

ИСО/МЭК 17799:2005, Information technology — Security techniques — Code of practice for information security management [ISO/IEC 17799:2005, Информационная технология – Методы и средства обеспечения безопасности – Практическое руководство по управлению информационной безопасностью]

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 Анализ рисков (risk analysis): Систематическое использование информации для идентификации источников возникновения и оценки рисков. [ISO/IEC Guide 73:2002]

3.2 Доступность (availability): Свойство быть доступным и готовым к использованию по требованию авторизованного пользователя (сущности) [ISO/IEC 13335-1:2004]

3.3 Информационная безопасность (information security): Обеспечение конфиденциальности, целостности и доступности информации; кроме того, могут также вовлекаться другие свойства, такие как подлинность (authenticity), подотчетность (accountability), неотказуемость (non-repudiation) и надежность (reliability). [ISO/IEC 17799:2005]

3.4 Инцидент информационной безопасности (information security incident): Единичное событие или ряд нежелательных и непредвиденных событий информационной безопасности, из-за которых велика вероятность компрометации бизнес-информации и реализации угрозы информационной безопасности. [ISO/IEC TR 18044:2004]

3.5 Конфиденциальность (confidentiality): Свойство, что информация становится недоступной и не раскрывается для неавторизованных пользователей, сущностей или процессов. [ISO/IEC 13335-1:2004]

3.6 Обработка риска (risk treatment): Процесс выбора и применения мер для изменения риска. [ISO/IEC Guide 73:2002]

Примечание. В настоящем стандарте термин «средство управления» (control) используется как синоним термина «мера» (measure).

3.7 Определение уровня риска (risk evaluation): Процесс сравнения оцененного риска с заданными критериями для определения значимости риска. [ISO/IEC Guide 73:2002]

3.8 Остаточный риск (residual risk): Риск, остающийся после обработки риска. [ISO/IEC Guide 73:2002]

3.9 Оценка рисков (risk assessment): Полный процесс, включающий в себя анализ рисков и определение уровня рисков. [ISO/IEC Guide 73:2002]

3.10 Положение о применимости (statement of applicability): Документ, описывающий цели управления и средства управления, которые признаны значимыми и применимыми к СУИБ организации.

Примечание. Цели управления и средства управления основываются на результатах и выводах, полученных из процессов оценки рисков и обработки рисков, правовых и нормативных требованиях, договорных обязательствах и бизнес-требованиях организации к информационной безопасности.

3.11 Принятие риска (risk acceptance): Решение по принятию риска. [ISO/IEC Guide 73:2002]

3.12 Ресурс (asset): Любая сущность, представляющая ценность для организации [ISO/IEC 13335-1:2004]

3.13 Система управления информационной безопасностью, СУИБ (information security management system - ISMS): Часть общей системы управления, основанная на оценке бизнес-рисков и предназначенная для разработки, реализации, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности.

Примечание. Система управления включает в себя организационную структуру, политики, разработку планов, распределение ответственности, инструкции, процедуры, процессы и ресурсы.

3.14 Событие информационной безопасности (information security event): Идентифицированный случай состояния системы или сети, указывающий на возможное нарушение политики информационной безопасности или отказ средств защиты (safeguards), либо ранее неизвестная ситуация, которая может быть существенной для безопасности. [ISO/IEC TR 18044:2004]

3.15 Управление рисками (risk management): Скоординированные действия, направленные на руководство и управление организацией с учетом существующих рисков. [ISO/IEC Guide 73:2002]

3.16 Целостность (integrity): Свойство сохранения точности и полноты ресурсов. [ISO/IEC 13335-1:2004]

4 Система управления информационной безопасностью

4.1 Общие требования

Организация должна разработать, реализовать, эксплуатировать, вести мониторинг и анализ, осуществлять сопровождение и совершенствование документированной СУИБ в контексте общей бизнес-деятельности организации и рисков, с которыми она сталкивается. Процесс, используемый для целей настоящего стандарта, основывается на модели ПРОК, представленной на рисунке 1.

4.2 Разработка и управление СУИБ

4.2.1 Разработка СУИБ

Организация должна выполнить следующее:

а) Определить область применения и границы СУИБ в терминах характеристик бизнеса, организации, ее местонахождения, ресурсов и технологий, при этом должно быть приведено подробное обоснование для всех исключений из области применения (см. 1.2).

б) Определить политику СУИБ в терминах характеристик бизнеса, организации, ее местонахождения, ресурсов и технологий. Эта политика:

1) включает в себя общую структуру для определения целей, а также определяет общие задачи руководства и принципы деятельности с учетом информационной безопасности;

2) учитывает производственные и правовые или нормативные требования, а также договорные обязательства;

3) учитывает контекст управления стратегическими рисками организации, в котором будут осуществляться разработка и сопровождение СУИБ;

4) устанавливает критерии, по которым будет определяться уровень рисков (см. 4.2.1в));

5) утверждается руководством.

Примечание. Для целей настоящего стандарта политика СУИБ рассматривается как надмножество (расширенное множество) политики информационной безопасности. Эти политики могут быть описаны в одном документе.

в) Определить подход организации к оценке рисков.

1) Идентифицировать метод оценки рисков, который соответствует конкретной СУИБ, идентифицированным требованиям к безопасности бизнес-информации, а также правовым и нормативным требованиям.

2) Разработать критерии для принятия рисков и идентифицировать приемлемые уровни рисков (см. 5.1е).

Выбранный метод оценки рисков должен гарантировать сопоставимые и воспроизводимые результаты процедуры оценки рисков.

Примечание. Существуют различные методы оценки рисков. Примеры методов оценки рисков обсуждаются в стандарте ISO/IEC TR 13335-3, Information technology— Guidelines for the management of IT Security — Techniques for the management of IT Security (ISO/IEC TR 13335-3, Информационные технологии — Принципы управления безопасностью ИТ — Методы управления безопасностью ИТ).

г) Идентифицировать риски.

1) Идентифицировать ресурсы, относящиеся к области применения СУИБ, и владельцев[1] этих ресурсов.

2) Идентифицировать угрозы этим ресурсам.

3) Идентифицировать уязвимости, которые могут быть использованы для реализации этих угроз.

4) Идентифицировать воздействие, которое могут оказать на ресурсы нарушения конфиденциальности, целостности и доступности.

д) Проанализировать и оценить риски.

1) Оценить в масштабе организации воздействия на бизнес, которые могут оказать нарушения безопасности, принимая во внимание последствия нарушения конфиденциальности, целостности или доступности ресурсов.

2) Оценить реальную вероятность реализации нарушений безопасности в свете превалирующих угроз, уязвимостей и воздействий, связанных с этими ресурсами, а также реализованных на данный момент средств управления.

3) Оценить уровни рисков.

4) Определить, являются ли риски приемлемыми или требуют обработки, используя критерии принятия рисков, определенные в пункте в)2) 4.2.1.

е) Идентифицировать и оценить варианты обработки рисков.

К возможным действиям относятся:

1) применение надлежащих средств управления;

2) сознательное и намеренное принятие рисков, при условии, что они явно удовлетворяют политикам организации и критериям принятия рисков (см. в)2) 4.2.1);

3) предотвращение рисков;

4) передача ассоциированных бизнес-рисков другим сторонам, например, страховщикам и поставщикам.

ж) Выбрать цели управления и средства управления для обработки рисков.

---

[1] Термин «владелец» означает лицо или сущность, на которые возложена административная ответственность за управление эффективностью, развитием, сопровождением, использованием и безопасностью данных ресурсов. Термин «владелец» не подразумевает, что данное лицо действительно имеет право собственности на данные ресурсы.

Цели управления и средства управления должны быть выбраны и реализованы, чтобы удовлетворять требованиям, идентифицированным процессом оценки рисков и обработки рисков. При этом выборе должны учитываться критерии принятия рисков (см. в)2) 4.2.1), а также правовые и нормативные требования, договорные обязательства.

Частью этого процесса должен быть выбор целей управления и средств управления из Приложения А, в результате выбора должны удовлетворяться все идентифицированные требования.

Перечень целей управления и средств управления, приведенный в Приложении А, не является исчерпывающим, могут также быть выбраны дополнительные цели управления и средства управления.

Примечание – Приложение А содержит полный перечень целей управления и средств управления, которые, как правило, значимы в организациях. Пользователям настоящего стандарта предлагается ориентироваться на Приложение А как на отправную точку для выбора средств управления, чтобы гарантировать, что ни один из важных вариантов управления не остался невыявленным.

з) Получить у руководства утверждение предлагаемых остаточных рисков.

и) Получить разрешение руководства на реализацию и эксплуатацию СУИБ.

к) Подготовить Положение о применимости.

Должно быть подготовлено Положение о применимости, включающее в себя следующее:

1) Цели управления и средства управления, выбранные в **ж) 4.2.1**, а также причины их выбора;

2) Цели управления и средства управления, реализованные на текущий момент (см. **д)2) 4.2.1**);

3) Исключение любой из целей управления и любого из средств управления, перечисленных в Приложении А, а также обоснование исключения этих целей и средств.

Примечание. Положение о применимости дает сводку решений, касающихся обработки рисков. Обоснование исключений обеспечивает перекрестный контроль того, что ни одно из средств управления не было пропущено по недосмотру.

4.2.2 Реализация и эксплуатация СУИБ

Организация должна выполнить следующее:

а) Сформулировать положения плана обработки рисков, в котором идентифицируются соответствующие действия руководства, ресурсы, обязанности и приоритеты для управления рисками информационной безопасности (см. 5).

б) Реализовать план обработки рисков, чтобы достичь идентифицированных целей управления, что включает в себя рассмотрение вопросов финансирования, распределения ролей и ответственности.

в) Реализовать средства управления, выбранные в 4.2.1 ж), для выполнения целей 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. 4.2.3в)).

Примечание. Измерение эффективности средств управления позволяет менеджерам и персоналу определить, насколько успешно средства управления достигают запланированных целей управления.

д) Реализовать программы обучения и оповещения (см. **5.2.2**).

е) Управлять эксплуатацией СУИБ.

ж) Управлять ресурсами для СУИБ (см. **5.2**).

з) Реализовать процедуры и другие средства управления, позволяющие обеспечить незамедлительное обнаружение событий безопасности и реагирование на инциденты безопасности (см. **а) 4.2.3**).

4.2.3 Мониторинг и анализ СУИБ

Организация должна выполнить следующее:

а) Выполнять процедуры мониторинга и анализа процедур и других средств управления с целью:

1) своевременно обнаружить ошибки в результатах обработки;

2) своевременно идентифицировать неудавшиеся и успешные нарушения безопасности и инциденты безопасности;

3) предоставить руководству возможность определять, выполняются ли надлежащим образом действия по обеспечению безопасности, порученные людям или реализованные средствами информационных технологий;

4) помочь в выявлении событий безопасности и, таким образом, предотвратить инциденты безопасности путем использования индикаторов;

5) 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.

в) Измерять эффективность средств управления, чтобы убедиться в том, что требования безопасности удовлетворяются.

г) Осуществлять анализ оценок рисков через запланированные периоды и анализировать уровень остаточных рисков и идентифицированные приемлемые уровни рисков с учетом изменений, происходящих в:

1) организации;
2) технологии;
3) бизнес-целях и бизнес-процессах;
4) идентифицированных угрозах;
5) эффективности реализованных средств управления;
6) внешних событиях, таких, как изменения в правовой или нормативной области, изменения договорных обязательств и изменения в общественном климате.

д) Проводить внутренние аудиты СУИБ через запланированные периоды времени (см. 6).

Примечание. Внутренние аудиты, иногда именуемые аудитами первой стороны, выполняются силами самой организации или по поручению организации для внутренних целей.

е) Регулярно проводить анализ СУИБ управленческим персоналом, чтобы гарантировать, что область применения остается адекватной, а усовершенствования процесса СУИБ идентифицированы (см. **7.1**).

ж) Обновлять планы по безопасности, чтобы 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**).

4.2.4 Сопровождение и совершенствование СУИБ

Организация должна регулярно выполнять следующее:

а) Реализовывать идентифицированные усовершенствования СУИБ.

б) Принимать надлежащие корректирующие и превентивные меры в соответствии с пп. 8.2 и 8.3. Применять знания, полученные 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, если этого требует значимость и важность таких действий.

г) Удостоверяться, что усовершенствования достигают поставленных целей.

4.3 Требования к документации

4.3.1 Общие требования

Документация должна включать в себя записи управленческих решений, гарантировать прослеживаемость связи действий с управленческими решениями и политиками, а также обеспечивать воспроизводимость записанных результатов.

Важно, чтобы имелась возможность продемонстрировать взаимосвязи от выбранных средств управления назад к результатам оценки рисков и процесса обработки рисков, и далее до политики СУИБ и целей.

Документация по СУИБ должна включать:

а) документированные положения политики безопасности (см. б) 4.2.1) и цели управления;

б) область применения СУИБ (см. а) 4.2.1);

в) процедуры и средства управления, используемые для поддержки СУИБ;

г) решение о методе оценки рисков (см. в) 4.2.1);

д) отчет об оценке рисков (см. в) и ж) 4.2.1);

е) план обработки рисков (см. б) 4.2.2);

ж) документированные процедуры, необходимые организации для обеспечения эффективного планирования, эксплуатации и управления своими процессами информационной безопасности и для описания способа измерения эффективности средств управления (см. в) 4.2.3);

з) записи, требуемые настоящим стандартом (см. 4.3.3).

и) Положение о применимости.

Примечание 1. В настоящем стандарте термин «документированная процедура» означает, что эта процедура разработана, задокументирована, реализована и поддерживается.

Примечание 2. Объем документации по СУИБ может отличаться от организации к организации в зависимости от:

1 Размера организации и вида ее деятельности;

2 Области применения и сложности требований к безопасности и управляемой системы.

Примечание 3. Документы и записи могут быть на носителе любого типа.

4.3.2 Управление документами

Документы, необходимые для СУИБ, должны быть защищенными и управляемыми. Должна быть разработана документированная процедура для определения управляющих воздействий, необходимых для:

а) утверждения документов по критерию их адекватности перед публикацией документов;

б) анализа и обновления документов по мере необходимости и повторного утверждения документов;

в) обеспечения идентификации изменений и статуса текущей редакции документов;

г) обеспечения доступности важных версий соответствующих документов в местах их использования;

д) сохранения удобочитаемости и быстрой идентификации документов;

е) обеспечения доступности документов для тех, кому они требуются, а также передачи, хранения и, наконец, уничтожения документов согласно процедурам, применяемым в соответствии с классификацией документов.

ж) обеспечения идентификации документов внешнего происхождения;

з) обеспечения контроля над распространением документов;

и) предотвращения случайного использования устаревших документов;

к) применения удобной идентификации документов, если они сохраняются для каких-либо целей.

4.3.3 Управление записями

Должны быть созданы и поддерживаться записи, обеспечивающие свидетельства соответствия требованиям и эффективной эксплуатации СУИБ. Записи должны быть защищенными и управляемыми. СУИБ должна учитывать все важные правовые и нормативные требования, а также договорные обязательства. Записи должны быть удобочитаемыми, легко идентифицируемыми и извлекаемыми. Должны быть документированы и реализованы средства управления, необходимые для идентификации, хранения, защиты, извлечения и уничтожения записей, а также срок хранения записей.

Должны вестись записи производительности процесса, как описано в п. 4.2, и записи всех случаев важных инцидентов безопасности, связанных с СУИБ.

Пример. Примерами записей являются журнал посещений, отчеты об аудите и заполненные формы разрешения доступа.

5 Распределение обязанностей персонала

5.1 Приверженность руководства

Руководство должно продемонстрировать свою приверженность (заинтересованность) к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ посредством:

а) утверждения политики СУИБ;

б) удостоверения того, что цели и планы СУИБ определены;

в) утверждения ролей и ответственности за информационную безопасность;

г) информирования организации о важности достижения целей информационной безопасности и соблюдения политики информационной безопасности, ответственности организации перед законом и необходимости постоянного совершенствования;

д) предоставления достаточные ресурсов для разработки, реализации, эксплуатации сопровождения и совершенствования СУИБ (см. п. 5.2.1);

е) выбора критериев для принятия рисков и приемлемых уровней рисков;

ж) обеспечения проведения внутренних аудитов СУИБ (см. п. 6);

з) проведения управленческого анализа СУИБ (см. п. 7).

5.2 Управление ресурсами

5.2.1 Предоставление ресурсов

Организация должна определить и предоставить ресурсы, необходимые для:

а) разработки, реализации, эксплуатации, мониторинга, анализа, сопровождения и совершенствования СУИБ;

б) обеспечения поддержки бизнес-требований процедурами информационной безопасности;

в) идентификации и учета правовых и нормативных требований, а также договорных обязательств по безопасности;

г) обеспечения адекватной безопасности с помощью корректного применения всех реализованных средств управления;

д) выполнения анализа по мере необходимости и надлежащего реагирования по результатам анализа;

е) совершенствования, если требуется, эффективности СУИБ.

5.2.2 Обучение, осведомленность и компетентность

Организация должна гарантировать, что весь персонал, на который возложены обязанности, определенные в СУИБ, имеет надлежащую квалификацию для выполнения необходимых задач. Для этого организация должна:

а) определить необходимый уровень квалификации персонала, выполняющего работы, связанные с СУИБ;

б) обеспечить обучение или принять другие меры (например, нанять квалифицированный персонал) для удовлетворения этих потребностей;

в) оценить эффективность принятых мер;

г) вести записи об образовании, обучении, навыках, опыте и квалификации (см. п. 4.3.3).

Организация должна также гарантировать, что весь задействованный персонал осведомлен о значимости и важности его деятельности по обеспечению информационной безопасности, а также о том, каким образом этот персонал участвует в достижении целей СУИБ.

6 Внутренние аудиты СУИБ

Организация должна проводить внутренние аудиты СУИБ через запланированные интервалы, чтобы определить, обладают ли цели

управления, средства управления, процессы и процедуры СУИБ следующими качествами:

а) удовлетворяют требованиям настоящего стандарта и соответствующим законам и нормативам;

б) удовлетворяют идентифицированным требованиям информационной безопасности;

в) являются эффективно реализованными и сопровождаемыми;

г) выполняются в соответствии с ожиданиями.

Программа аудита должна быть спланирована с учетом статуса и важности процессов и областей, подлежащих аудиту, а также с учетом результатов предыдущих аудитов. Должны быть определены критерии, границы, периодичность и методы аудита. Выбор аудиторов и проведение аудитов должны гарантировать объективность и беспристрастность процесса аудита. Аудиторы не должны проводить аудит своей собственной работы.

Обязанности и требования к планированию и проведению аудита, а также к отчетности по результатам аудита и ведению записей (см. п. 4.3.3) должны быть определены в документированной процедуре.

Управленческий персонал, ответственный за подлежащую аудиту область, должен обеспечить незамедлительное принятие мер для устранения обнаруженных несоответствий и их причин. Последующие действия должны включать в себя проверку принятых мер и отчет по результатам проверки (см. п. 8).

Примечание. Стандарт ISO 19011:2002, Guidelines for quality and/or environmental management systems, содержит полезное руководство по проведению внутренних аудитов СУИБ.

7 Пересмотр СУИБ руководством

7.1 Общие положения

Управленческий персонал должен через запланированные интервалы (не реже раза в год) анализировать СУИБ организации, чтобы обеспечить ее постоянную применимость, адекватность и эффективность. Этот анализ должен включать в себя определение возможностей совершенствования и необходимости изменения СУИБ, в том числе политики информационной безопасности и целей информационной безопасности. Результаты анализа должны быть задокументированы в явном виде, а также должны вестись соответствующие записи (см. п. 4.3.3).

7.2 Исходные данные для анализа

Исходные данные для управленческого анализа должны включать в себя:

а) результаты аудитов и анализа СУИБ;

б) замечания и предложения заинтересованных сторон;

в) информацию о методах, продуктах или процедурах, которые возможно использовать в организации для повышения производительности и эффективности СУИБ;

г) информацию о статусе превентивных и корректирующих мер;

д) информацию об уязвимостях или угрозах, не учтенных адекватно при предыдущей оценке рисков;

е) результаты измерения эффективности;

ж) информацию о мерах, принятых по результатам предыдущего управленческого анализа;

з) информацию обо всех изменениях, которые могли повлиять на СУИБ;

и) рекомендации по совершенствованию.

7.3 Итоги анализа

Итоги управленческого анализа должны включать в себя все решения и меры, связанные с перечисленным ниже.

а) Повышение эффективности СУИБ.

б) Обновление оценки рисков и плана обработки рисков.

в) Модификация, по мере необходимости, процедур и средств управления, воздействующих на информационную безопасность, для реагирования на внутренние и внешние события, которые могут повлиять на СУИБ, включая изменения в:

1) бизнес-требованиях;

2) требованиях безопасности;

3) бизнес-процессах, влияющих на существующие бизнес-требования;

4) нормативных или правовых требованиях;

5) договорных обязательствах;

6) уровнях риска и/или критериях принятия рисков.

г) Определение потребностей в ресурсах.

д) Совершенствование существующих способов измерения эффективности средств управления.

8 Совершенствование СУИБ

8.1 Постоянное совершенствование

Организация должна постоянно повышать эффективность СУИБ путем использования политики информационной безопасности, целей информационной безопасности, результатов аудита, анализа отслеживаемых событий, корректирующих и превентивных воздействий, а также управленческого анализа (см. п. 7).

8.2 Корректирующее воздействие

Организация должна принимать меры для устранения причин несоответствий требованиям СУИБ, чтобы предотвратить повторное появление несоответствий. Документированная процедура для корректирующего воздействия должна определять требования к:

а) идентификации несоответствий;

б) определению причин несоответствий;

в) оценке необходимости воздействий, исключающих возможность повторного появления несоответствий;

г) определению и реализации необходимых корректирующих воздействий;

д) регистрации результатов предпринятых воздействий (см. п. 4.3.3);

е) анализу предпринятых корректирующих воздействий.

8.3 Превентивное воздействие

Организация должна определить меры для исключения причин возможных несоответствий требованиям СУИБ, чтобы предотвратить появление несоответствий. Принимаемые превентивные меры должны быть адекватны воздействию потенциальных проблем. Документированная процедура для превентивного воздействия должна определять требования к:

а) идентификации потенциальных несоответствий и их причин;

б) оценке необходимости воздействия для предотвращения появления несоответствий;

в) определению и реализации необходимого превентивного воздействия;

г) регистрации результатов предпринятого воздействия (см. п. 4.3.3);

д) анализу предпринятого превентивного воздействия.

Организация должна идентифицировать изменившиеся риски и идентифицировать требования к превентивным воздействиям, уделяя особое внимание значительно изменившимся рискам.

Приоритет превентивных воздействий должен определяться на основании результатов оценки рисков.

Примечание. Действие по предотвращению несоответствий часто является более дорогостоящим, чем корректирующее воздействие.

Приложение А
(рекомендуемое)
Цели управления и средства управления

Цели управления и средства управления, перечисленные в Таблице А.1, получены непосредственно из и находятся в соответствии с целями и средствами, перечисленными в пунктах с **5** по **15** стандарта ИСО/МЭК 17799:2005. Перечни в Таблице А.1 не являются исчерпывающими, и организация может счесть необходимым использование дополнительных целей управления и средств управления. Цели управления и средства управления из этих таблиц должны быть выбраны как часть процесса СУИБ, определенного в п. **4.2.1**.

Пункты **5–15** стандарта ИСО/МЭК 17799:2005 содержат рекомендации по реализации и руководство по практическому применению средств управления, описанных в пунктах **А.5**–**А.15**.

Таблица А.1. Цели управления и средства управления

А.5 Политика безопасности		
А.5.1 Политика информационной безопасности Цель: Обеспечить для информационной безопасности управление и поддержку со стороны управленческого персонала согласно бизнес-требованиям и соответствующим законам и нормативам.		
А.5.1.1	Документ о политике информационной безопасности	Средство управления Документ о политике информационной безопасности должен быть утвержден руководством организации, опубликован и доведен до сведения всех сотрудников и релевантных внешних сторон.
А.5.1.2	Анализ политики информационной безопасности	Средство управления Политика информационной безопасности должна анализироваться через запланированные интервалы 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 Цель: Управлять информационной безопасностью в организации.		
А.6.1.1	Заинтересованность руководства в информационной безопасности	Средство управления Руководство должно активно поддерживать безопасность в организации путем прямого указания, демонстрации заинтересованности, прямого назначения и признания ответственности за информационную безопасность.
А.6.1.2	Координация информационной безопасности	Средство управления Деятельность по информационной безопасности должна быть скоординирована представителями различных частей организации с соответствующими ролями и рабочими функциями.
А.6.1.3	Распределение обязанностей по обеспечению информационной безопасности	Средство управления Должны быть четко определены обязанности по обеспечению информационной безопасности.
А.6.1.4	Процесс утверждения средств обработки информации	Средство управления Должен быть определен и реализован процесс утверждения руководством новых средств обработки.

A.6.1.5	Соглашения о конфиденциальности	Должны быть идентифицированы и должны регулярно пересматриваться требования к соглашениям о конфиденциальности или неразглашении, отражающие потребности организации в защите информации.
A.6.1.6	Контакт с уполномоченными организациями	Средство управления Должны поддерживаться надлежащие контакты с соответствующими организациями.
A.6.1.7	Контакт со специализированными группами	Средство управления Должен поддерживаться надлежащий контакт со специализированными группами или другими форумами специалистов по информационной безопасности и профессиональными объединениями.
A.6.1.8	Независимый анализ информационной безопасности	Средство управления Подход организации к управлению информационной безопасностью и его реализация (т.е. цели управления, средства управления, политики, процессы и процедуры информационной безопасности) должны подвергаться независимому анализу через запланированные интервалы времени или в случае значительных изменений в реализации безопасности.
A.6.2 Внешние организационные аспекты Цель: Обеспечить безопасность информации и средств обработки информации организации, которые доступны, обрабатываются, известны или управляются сторонними организациями.		
A.6.2.1	Идентификация рисков, связанных со сторонними организациями	Средство управления Риски для информации и средств обработки информации организации, возникающие в бизнес-процессах, в которые вовлечены внешние организации, должны быть идентифицированы и должны быть реализованы надлежащие средства управления до того, как к этой информации и средствам будет предоставлен доступ.
A.6.2.2	Обеспечение безопасности при работе с заказчиками	Средство управления Все идентифицированные требования безопасности должны быть выполнены до того, как заказчикам будет предоставлен доступ к информации или ресурсам организации.
A.6.2.3	Обеспечение безопасности в соглашениях со сторонними организациями	Средство управления Соглашения со сторонними организациями, предусматривающие доступ, обработку, использование, управление информацией или средствами обработки информации организации либо добавление продуктов или сервисов в средства обработки информации, должны учитывать все требования безопасности, относящиеся к предмету соглашения.
A.7 Управление ресурсами		
A.7.1 Ответственность за ресурсы Цель: Обеспечить и поддерживать надлежащую защиту ресурсов организации.		
A.7.1.1	Инвентаризация ресурсов	Средство управления Все ресурсы должны быть в актуальном состоянии идентифицированы, должна быть составлена и поддерживаться в актуальном состоянии опись всех важных ресурсов.

A.7.1.2	Владение ресурсами	Средство управления Вся информация и ресурсы, связанные со средствами обработки информации, должны быть «во владении»[2] уполномоченного подразделения организации.
A.7.1.3	Допустимое использование ресурсов	Средство управления Должны быть идентифицированы, документированы и реализованы правила допустимого использования информации и ресурсов, связанных со средствами обработки информации.
A.7.2 Классификация информации Цель: Гарантировать, что обеспечен надлежащий уровень защиты информации.		
A.7.2.1	Рекомендации по классификации	Средство управления Информация должна быть классифицирована по таким показателям, как значимость, правовые требования, чувствительность к воздействиям и критичность для организации.
A.7.2.2	Маркировка и обращение с информацией	Средство управления Должен быть разработан и реализован в соответствии с принятой в организации системой классификации надлежащий набор процедур для маркировки и обращения с информацией.
A.8 Аспекты безопасности, связанные с персоналом		
A.8.1 До работы[3] Цель: 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.		
A.8.1.1	Роли и сферы ответственности	Средство управления Роли безопасности и ответственность сотрудников, подрядчиков и пользователей их сторонних организаций должны быть определены и документированы в соответствии с политикой информационной безопасности организации.
A.8.1.2	Проверка принимаемых на работу	Средство управления Проверки персональных данных всех кандидатов на вакансии, подрядчиков и пользователей из сторонних организаций должны выполняться согласно соответствующим законам, нормативным документам и этическим нормам, а также с учетом бизнес-требований, категории информации, к которой будет предоставлен доступ, и осознаваемым рискам.
A.8.1.3	Постановления и условия найма	Средство управления Как часть своих контрактных обязательств сотрудники, подрядчики и пользователей из сторонних организаций должны принять и подписать постановления и условия своего контракта о найме, которые должны устанавливать их ответственность и ответственность организации за информационную безопасность.

[2] Пояснение: Термин «владелец» означает лицо или сущность, на которые возложена административная ответственность за управление эффективностью, развитием, сопровождением, использованием и безопасностью данных ресурсов. Термин «владелец» не подразумевает, что данное лицо действительно имеет право собственности на данные ресурсы.

[3] Пояснение: Термин «найм» используется здесь для обозначения всех следующих ситуаций: найм персонала (временного или постоянного), назначение рабочих ролей, изменение рабочих ролей, переуступка контрактов, истечение срока действия любого из перечисленных соглашений.

A.8.2 Во время найма Цель: 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.		
A.8.2.1	Ответственность руководства	Средство управления Руководство должно требовать, чтобы сотрудники, подрядчики и пользователи из сторонних организаций применяли правила информационной безопасности в соответствии с установленными в организации политиками и процедурами.
A.8.2.2	Осведомленность, обучение и компетентность в области информационной безопасности	Средство управления Все сотрудники организации и, где необходимо, подрядчики и пользователи из сторонних организаций должны получить надлежащее осведомляющее обучение и регулярно получать информацию об обновлениях политик и процедур организации, в объеме, необходимом для выполнения ими своих рабочих функций.
A.8.2.3	Дисциплинарный процесс	Средство управления Должен быть определен формальный дисциплинарный процесс для сотрудников, которые нарушили безопасность.
A.8.3 Увольнение или изменение условий найма Цель: Гарантировать, что сотрудники, подрядчики и пользователи из сторонних организаций покидают организацию или изменяют условия найма в установленном порядке.		
A.8.3.1	Ответственность за увольнение	Средство управления Ответственность за выполнение процедур увольнения сотрудников или изменения условий найма должна быть определена и назначена.
A.8.3.2	Возвращение ресурсов	Средство управления Все сотрудники, подрядчики и пользователи из сторонних организаций должны вернуть все ресурсы организации, находившиеся в их распоряжении, до даты увольнения или окончания срока действия контракта (соглашения).
A.8.3.3	Прекращение прав доступа	Средство управления Права доступа всех сотрудников, подрядчиков и пользователей из сторонних организаций к информации и средствам обработки информации должны либо аннулироваться в случае увольнения, прекращения контракта или соглашения, либо изменяться в соответствии с измененными условиями найма.
A. 9 Физическая безопасность и безопасность среды функционирования		
A.9.1 Защищенные области Цель: Предотвратить несанкционированный физический доступ, ущерб или влияние на территорию, оборудование и информацию организации.		
A.9.1.1	Физический периметр безопасности	Средство управления Для защиты областей, в которых находится информация и средства обработки информации, должны использоваться периметры безопасности (барьеры, такие как стены, вход, оборудованный системой пропуска по картам, или контроль входящих специальным персоналом).
A.9.1.2	Контроль доступа в помещения	Средство управления Защищаемые области должны быть защищены необходимыми средствами контроля доступа в помещения, чтобы обеспечить доступ к ним только персонала, получивший соответствующие полномочия.

A.9.1.3	Защита офисов, комнат и оборудования	Средство управления Для защиты офисов, комнат и оборудования должны быть разработаны и внедрены меры физической безопасности
A.9.1.4	Защита от внешних угроз и угроз окружающей среды	Средство управления Должны быть разработаны и внедрены меры физической защиты от пожара, затопления, землетрясения, взрыва, гражданских беспорядков и других форм природных и антропогенных катастроф.
A.9.1.5	Работа в защищенных областях	Средство управления Должны быть разработаны и внедрены меры физической защиты и принципы работы в защищенных областях.
A.9.1.6	Места свободного доступа, разгрузки и погрузки	Средство управления Места свободного доступа, такие как площадки для разгрузки и погрузки и другие места, куда возможен доступ неуполномоченных лиц, должны контролироваться и, при возможности, должны изолироваться от средств обработки информации в целях предотвращения несанкционированного доступа.
A.9.2 Защита оборудования Цель: Предотвратить потерю, повреждение, кражу или компрометацию ресурсов, а также перебои в деятельности организации		
A.9.2.1	Размещение и защита оборудования	Средство управления Оборудование должно быть размещено или защищено так, чтобы уменьшить риски и ущерб, связанные с воздействием внешней среды, а также вероятность несанкционированного доступа.
A.9.2.2	Поддерживающая инфраструктура	Средство управления Оборудование должно быть защищено от сбоев в системе электропитания и других неполадок, возникающих из-за сбоев в поддерживающей инфраструктуре.
A.9.2.3	Защита кабельной сети	Средство управления Кабельные системы электропитания и телекоммуникаций, используемые для передачи данных или поддержки информационных сервисов, должны быть защищены от прослушивания или повреждения.
A.9.2.4	Сопровождение оборудования	Средство управления Должно обеспечиваться надлежащее сопровождение оборудования, чтобы гарантировать его постоянную доступность и целостность.
A.9.2.5	Безопасность оборудования за пределами организации	Средство управления К оборудованию за пределами организации должны применяться меры безопасности, учитывающие различные риски работы вне территории организации.
A.9.2.6	Надежная утилизация или повторное использование оборудования	Средство управления Перед утилизацией все единицы оборудования, содержащие носители информации, должны проверяться, чтобы гарантировать, что все критичные данные и лицензионное программное обеспечение удалено с них или надежно замещено другой информацией.
A.9.2.7	Перемещение собственности	Средство управления Оборудование, информация или программное обеспечение не должны выноситься за пределы организации без соответствующей санкции руководства.
A.10 Управление коммуникациями и функционированием		
A.10.1 Операционные процедуры и ответственность Цель: Обеспечить корректное и защищенное функционирование средств обработки информации.		

A.10.1.1	Документированные операционные процедуры	Средство управления Операционные процедуры должны быть задокументированы, должно быть обеспечено их сопровождение, а также доступность для всех пользователей, которым они требуются.
A.10.1.2	Управление изменениями	Средство управления Изменения в средствах и системах обработки информации должны контролироваться.
A.10.1.3	Разделение обязанностей	Средство управления Обязанности и зоны ответственности должны быть разделены для уменьшения вероятности несанкционированной или непреднамеренной модификации или ненадлежащего использования ресурсов организации.
A.10.1.4	Разделение средств разработки, тестирования и производственных средств	Средство управления Средства разработки, тестирования и производственные средства должны быть разделены для уменьшения рисков несанкционированного доступа или изменений операционной системы.
A.10.2 Управление предоставлением сервисов сторонних организаций Цель: Реализовать и поддерживать надлежащий уровень информационной безопасности и предоставления сервисов в соответствии с соглашением о поставке сервисов сторонней организацией.		
A.10.2.1	Предоставление сервиса	Средство управления Должно быть гарантировано, 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	Мониторинг и анализ сервисов сторонних организаций	Средство управления Сервисы, отчеты и записи, предоставляемые сторонней организацией, должны регулярно подвергаться мониторингу и анализу, кроме того, должны регулярно производиться аудиты.
A.10.2.3	Управление изменениями в сервисах сторонних организаций	Средство управления Изменения в предоставлении сервисов, включая сопровождение и совершенствование существующих политик информационной безопасности, процедур и средств управления, должны управляться с учетом критичности вовлеченных бизнес-систем и процессов, а также повторной оценки рисков.
A.10.3 Планирование систем и их приемка Цель: Минимизировать риск отказов систем.		
A.10.3.1	Планирование нагрузки	Средство управления Использование ресурсов должно отслеживаться (мониторинг) и приводиться в соответствие, должны составляться прогнозы будущих потребностей, чтобы обеспечить необходимую производительность системы.
A.10.3.2	Приемка систем	Средство управления Критерии приемки новых информационных систем, модернизаций и новых версий должны быть установлены, и должно быть выполнено надлежащее тестирование системы во время ее разработки, но до приемки системы.
A.10.4 Защита от вредоносного и мобильного программного кода Цель: Обеспечить целостность программного обеспечения и информации.		

A.10.4.1	Средства защиты от вредоносного программного кода	Средство управления Должны быть реализованы средства обнаружения, предотвращения и восстановления, обеспечивающие защиту от вредоносного программного кода, а также надлежащие процедуры оповещения пользователей.
A.10.4.2	Средства защиты от мобильного кода	Средство управления Там, где разрешено использование мобильного кода, конфигурация должна гарантировать, что санкционированный мобильный код функционирует в соответствии с явно заданной политикой безопасности, а исполнение несанкционированного мобильного кода не допускается.
A.10.5 Резервное копирование		
A.10.5.1	Резервное копирование информации	Средство управления Резервные копии информации и программного обеспечения должны создаваться и тестироваться регулярно, в соответствии с установленной политикой резервного копирования.
A.10.6 Управление безопасностью сетей Цель: Обеспечить защиту информации в сетях и защиту поддерживающей инфраструктуры.		
A.10.6.1	Средства управления сетью	Средство управления Сети должны надлежащим образом управляться и контролироваться, чтобы быть защищенными от угроз и чтобы поддерживать безопасность систем и приложений, используемых сетью, включая информацию, передаваемую по сетям.
A.10.6.2	Безопасность сетевых сервисов	Средство управления Средства безопасности, уровень сервисов и требования по управлению для всех сетевых сервисов должны быть идентифицированы и включены во все соглашения относительно сетевых сервисов, независимо от того, предоставляются ли эти сервисы силами самой организации или внешними организациями (аутсорсинг).
A.10.7 Управление носителями информации и их защита Цель: Предотвратить повреждение информационных ресурсов и приостановку работы организации.		
A.10.7.1	Управление съемными носителями информации	Средство управления Должны быть установлены процедуры управления съемными носителями информации.
A.10.7.2	Уничтожение носителей информации	Средство управления Носители информации, которые больше не нужны, должны быть уничтожены безопасным и надежным способом, с соблюдением формальных процедур.
A.10.7.3	Процедуры обращения с информацией	Средство управления Должны быть установлены процедуры обращения с информацией и хранения информации, чтобы защитить информацию от несанкционированного раскрытия или ненадлежащего использования.
A.10.7.4	Защита системной документации	Средство управления Системная документация должна быть защищена от несанкционированного доступа.
A.10.8 Обмен информацией Цель: Обеспечить безопасность информации и программного обеспечения, которые являются предметом информационного обмена как внутри организации, так и с любыми внешними объектами.		

A.10.8.1	Политики и процедуры информационного обмена	Средство управления Формальные политики и процедуры обмена, а также средства обмена должны быть установлены для защиты обмена информацией с использованием средств коммуникации всех типов.
A.10.8.2	Соглашения об обмене	Средство управления Должны быть заключены соглашения об обмене информацией и программным обеспечением между организацией и внешними организациями.
A.10.8.3	Транспортировка физических носителей информации	Средство управления Во время транспортировки за пределами территории организации содержащие информацию носители должны быть защищены от несанкционированного доступа, ненадлежащего использования или повреждения.
A.10.8.4	Электронные сообщения	Средство управления Информация, циркулирующая в системах обмена электронными сообщениями, должна быть надлежащим образом защищена.
A.10.8.5	Информационные системы бизнеса	Средство управления Должны быть разработаны и реализованы политики и процедуры для защиты информации, связанной с объединением информационных систем бизнеса.
A.10.9 Сервисы электронной коммерции Цель: Обеспечить безопасность сервисов электронной коммерции, а также их безопасное использование.		
A.10.9.1	Электронная коммерция	Средство управления Информация, используемая в электронной коммерции и проходящая через общедоступные сети, должна быть защищена от мошеннических действий, споров по контрактам, несанкционированного разглашения и модификации.
A.10.9.2	Операции в реальном времени (он-лайн)	Средство управления Информация, используемая в операциях он-лайн, должна быть защищена, чтобы предотвратить неполную передачу, неверную маршрутизацию, несанкционированную замену сообщений, несанкционированное разглашение, несанкционированное дублирование или воспроизведение сообщений.
A.10.9.3	Общедоступная информация	Средство управления Целостность информации, циркулирующей в общедоступных системах, должна быть защищена для предотвращения несанкционированной модификации.
A.10.10 Мониторинг Цель: Обнаружить несанкционированные действия по обработке информации.		
A.10.10.1	Ведение журналов аудита	Средство управления Журналы аудита, регистрирующие действия пользователей, исключительные ситуации и события информационной безопасности, должны вестись и храниться в течение установленного периода, чтобы помочь в будущих обследованиях и мониторинге управления доступом.
A.10.10.2	Мониторинг использования системы	Средство управления Должны быть установлены процедуры мониторинга использования средств обработки информации, а результаты мониторинга должны регулярно анализироваться.

A.10.10.3	Защита информации журналов	Средство управления Средства ведения журналов и информация журналов должны быть защищены от тайных воздействий и несанкционированного доступа.
A.10.10.4	Журналы администратора и оператора	Средство управления Действия системного администратора и оператора системы должны регистрироваться в соответствующих журналах.
A.10.10.5	Регистрация сбоев	Средство управления Сбои должны быть зарегистрированы в журнале, проанализированы, и по ним должны быть приняты соответствующие меры.
A.10.10.6	Синхронизация системных часов	Средство управления Часы всех важных систем обработки информации в рамках организации или домена безопасности должны быть синхронизированы по установленному источнику точного времени.
A.11 Управление доступом		
A.11.1 Бизнес-требования к управлению доступом Цель: Управление доступом к информации.		
A.11.1.1	Политика управления доступом	Средство управления Политика управления доступом должна быть установлена, документирована и пересматриваться с учетом требований к доступу со стороны бизнеса и безопасности.
A.11.2 Управление доступом пользователей Цель: Обеспечить санкционированный доступ пользователей и предотвратить несанкционированный доступ к информационным системам.		
A.11.2.1	Регистрация пользователей	Средство управления Должна быть установлена формальная процедура регистрации и отмены регистрации пользователей для предоставления и аннулирования доступа ко всем информационным системам и сервисам.
A.11.2.2	Управление полномочиями	Средство управления Предоставление и использование полномочий должно быть ограниченным и контролируемым.
A.11.2.3	Управление паролями пользователей	Средство управления Назначение паролей должно контролироваться посредством формального процесса управления.
A.11.2.4	Пересмотр прав доступа пользователей	Средство управления Руководство должно пересматривать права доступа пользователей через регулярные интервалы времени, используя формальный процесс.
A.11.3 Ответственность пользователей Цель: Предотвратить несанкционированный доступ пользователей, а также компрометацию или кражу информации и средств обработки информации.		
A11.3.1	Использование паролей	Средство управления При выборе и использовании паролей пользователи должны придерживаться принципов безопасности, на практике доказавших свою эффективность.
A.11.3.2	Пользовательское оборудование, оставленное без присмотра	Средство управления Пользователи должны обеспечить надлежащую защиту оборудования, оставляемого без присмотра.

A.11.3.3	Политика «чистый стол» и «чистый экран	Средство управления Должна быть принята политика «чистый стол» для бумаг и съемных носителей информации и политика «чистый экран» для средств обработки информации.
A.11.4 Управление доступом к сети Цель: Предотвратить несанкционированный доступ к сетевым сервисам.		
A.11.4.1	Политика использования сетевых сервисов	Средство управления Пользователи должны получать доступ только к тем сервисам, использование которых им явным образом разрешено.
A.11.4.2	Аутентификация пользователей для внешних подключений	Средство управления Должны использоваться надлежащие методы аутентификации для контроля доступа удаленных пользователей.
A.11.4.3	Идентификация оборудования в сети	Средство управления Автоматическая идентификация оборудования должна рассматриваться как средство аутентификации соединений, устанавливаемых конкретными узлами и оборудованием.
A.11.4.4	Защита удаленного диагностического и конфигурационного порта	Средство управления Физический и логический доступ к диагностическим и конфигурационным портам должен контролироваться.
A.11.4.5	Разделение в сетях	Средство управления В сетях должны быть разделены (изолированы) группы информационных сервисов, пользователей и информационных систем
A.11.4.6	Управление сетевыми подключениями	Средство управления Для коллективно используемых сетей, особенно для тех, которые выходят за пределы организации, возможности пользователей по подключению к сети должны быть ограничены в соответствии с политикой управления доступом и требованиями бизнес-приложений (см. 11.1).
A.11.4.7	Управление сетевой маршрутизацией	Средство управления Средства управления маршрутизацией должны быть реализованы в сетях, чтобы гарантировать, что подключения компьютерных систем и информационные потоки не нарушают политику управления доступом бизнес-приложений.
A.11.5 Контроль доступа к операционной системе Цель: Предотвратить несанкционированный доступ к операционным системам.		
A.11.5.1	Безопасные процедуры входа	Средство управления Доступ к операционным системам должен контролироваться безопасной процедурой входа в систему.
A.11.5.2	Идентификация и аутентификация пользователей	Средство управления Все пользователи должны иметь уникальный идентификатор (ИД пользователя) только для личного использования, а также должен быть выбран подходящий метод аутентификации, чтобы подтверждать заявленную личность пользователя.
A.11.5.3	Система управления паролями	Средство управления Системы управления паролями должны быть интерактивными и должны обеспечивать качественные пароли.
A.11.5.4	Использование системных утилит	Средство управления Использование системных программ-утилит, с помощью которых можно изменить систему и средства управления приложениями, должно быть ограниченным и строго контролироваться.

A.11.5.5	Блокировка сеанса по времени	Средство управления Неактивные сеансы должны закрываться по истечении заданного времени бездействия.
A.11.5.6	Ограничение по времени подключения	Средство управления Ограничения по времени подключения должны использоваться для обеспечения дополнительной защиты приложений высокого риска
A.11.6 Управление доступом к приложениям и их информации Цель: Предотвратить несанкционированный доступ к информации, хранимой в информационных системах.		
A.11.6.1	Ограничение доступа к информации	Средство управления Доступ пользователей и обслуживающего персонала к информации и функциям прикладных систем должен ограничиваться в соответствии с заданной политикой управления доступом.
A.11.6.2	Изоляция критичных систем	Средство управления Критичные системы должны функционировать в выделенной (изолированной) вычислительной среде.
A.11.7 Мобильные вычисления и дистанционная работа (teleworking) Цель: Обеспечить информационную безопасность при использовании средств мобильных вычислений и дистанционной работы.		
A.11.7.1	Мобильные вычисления и коммуникации	Средство управления Должна существовать формальная политика и должны быть приняты надлежащие меры безопасности, чтобы обеспечить защиту от рисков, связанных с использованием средств мобильных вычислений и коммуникации.
A.11.7.2	Дистанционная работа	Средство управления Для дистанционной работы должны быть разработаны и реализованы политика, оперативные планы и процедуры.
A.12 Приобретение, разработка и сопровождение информационных систем		
A.12.1 Требования к безопасности информационных систем Цель: Гарантировать, что безопасность является компонентом информационных систем.		
A.12.1.1	Анализ и спецификация требований к безопасности	Средство управления Формулировки бизнес-требований к новым информационным системам или к модернизации существующих информационных систем должны устанавливать требования к средствам управления безопасностью.
A.12.2 Корректная обработка в приложениях Цель: Предотвратить ошибки, потерю, несанкционированную модификацию или ненадлежащее использование информации в приложениях.		
A.12.2.1	Проверка достоверности входных данных	Средство управления Должна производиться проверка достоверности входных данных приложений, чтобы гарантировать, что эти данные являются корректными и правильными.
A.12.2.2	Контроль внутренней обработки	Средство управления Проверки достоверности должны быть встроены в приложения, чтобы выявлять любые повреждения информации из-за ошибок обработки или умышленных действий.
A.12.2.3	Целостность сообщений	Средство управления Требование гарантирования аутентичности и защиты целостности сообщений в приложениях должно быть идентифицировано, и должны быть идентифицированы и реализованы соответствующие средства управления.

A.12.2.4	Проверка достоверности выходных данных	Средство управления Выходные данные приложения должны быть проверены на достоверность, чтобы гарантировать, что обработка хранимой информации корректна и соответствует текущим обстоятельствам.
A.12.3 Криптографические средства управления Цель: Обеспечить защиту конфиденциальности, аутентичности и целостности информации криптографическими средствами.		
A.12.3.1	Политика использования криптографических средств управления	Средство управления Должна быть разработана и реализована политика использования криптографических средств управления для защиты информации.
A.12.3.2	Управление ключами	Средство управления Управление ключами должно быть реализовано, чтобы поддерживать в организации использование криптографических методов.
A.12.4 Безопасность системных файлов Цель: Обеспечить безопасность системных файлов.		
A.12.4.1	Контроль производственного программного обеспечения	Средство управления Должны существовать процедуры контроля установки программного обеспечения в производственных системах.
A.12.4.2	Защита системных тестовых данных	Средство управления Тестовые данные должны тщательно выбираться, а также быть защищенными и контролируемыми.
A.12.4.3	Управление доступом к исходному коду программ	Средство управления Доступ к исходному коду программ должен быть ограничен.
A.12.5 Безопасность процессов разработки и технического обслуживания Цель: Поддерживать безопасность программного обеспечения и информации прикладных систем.		
A.12.5.1	Процедуры управления изменениями	Средство управления Реализация изменений должна контролироваться с помощью формальных процедур управления изменениями.
A.12.5.2	Технический анализ приложений после изменения производственной системы	Средство управления При изменении производственных систем критичные для бизнеса приложения должны быть проанализированы и протестированы, чтобы гарантировать отсутствие неблагоприятного воздействия на функционирование и безопасность организации.
A.12.5.3	Ограничения изменений пакетов программного обеспечения	Средство управления Модификации пакетов программного обеспечения не должны одобряться безоговорочно, модификации должны быть ограничены только необходимыми изменениями и все изменения должны строго контролироваться.
A.12.5.4	Утечка информации	Средство управления Должны быть предотвращены возможности для утечки информации.
A.12.5.5	Разработка программного обеспечения на условиях аутсорсинга	Средство управления Разработка программного обеспечения сторонними организациями (аутсорсинг) должна контролироваться и отслеживаться организацией.
A.12.6 Управление техническими уязвимостями Цель: Уменьшить риски, возникающие из-за использования опубликованных данных о технических уязвимостях.		

A.12.6.1	Управление техническими уязвимостями	Средство управления Информацию о технических уязвимостях информационных систем следует получать своевременно, незащищенность организации перед этими уязвимостями должна оцениваться, и должны приниматься адекватные меры для устранения рисков, связанных с такими уязвимостями.
A.13 Управление инцидентами информационной безопасности		
A.13.1 Составление отчетов о событиях информационной безопасности и слабостях защиты Цель: Гарантировать, что о событиях информационной безопасности и слабостях защиты, связанных с информационными системами, сообщается таким образом, что это позволяет своевременно принимать корректирующие меры.		
A.13.1.1	Сообщение о событиях информационной безопасности	Средство управления О событиях информационной безопасности должно сообщаться по надлежащим управленческим каналам как можно быстрее.
A.13.1.2	Сообщение о слабостях защиты	Средство управления Необходимо обязать всех сотрудников, подрядчиков и пользователей из сторонних организаций, использующих информационные системы и сервисы, отмечать и сообщать обо всех наблюдаемых или предполагаемых слабостях защиты систем или сервисов.
A.13.2 Управление инцидентами и совершенствованием информационной безопасности Цель: Гарантировать, что применяется непротиворечивый и эффективный подход к управлению инцидентами информационной безопасности.		
A.13.2.1	Ответственность и процедуры	Средство управления Должны быть установлены ответственность руководства и процедуры, чтобы обеспечить быстрое, эффективное и правильное реагирование на инциденты информационной безопасности.
A.13.2.2	Обучение на инцидентах информационной безопасности	Средство управления Должны быть реализованы механизмы, позволяющие измерять и отслеживать типы, объемы и стоимость инцидентов информационной безопасности.
A.13.2.3	Сбор доказательств	Средство управления 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), необходимо собрать, сохранить и представить доказательства, чтобы выполнить правила доказательства, установленные в соответствующем правоохранительном органе (органах).
A.14 Управление непрерывностью бизнеса		
A.14.1 Аспекты информационной безопасности в управлении непрерывностью бизнеса Цель: 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.		
A.14.1.1	Включение информационной безопасности в процесс управления непрерывностью бизнеса	Средство управления Должен быть разработан и поддерживается управляемый процесс обеспечения непрерывности бизнеса в рамках организации, который учитывает требования информационной безопасности, необходимые для непрерывности бизнеса данной организации.

A.14.1.2	Непрерывность бизнеса и оценка рисков	Средство управления Должны быть идентифицированы события, из-за которых возможны остановки бизнес-процессов, а также определены вероятность и воздействие таких остановок и их влияние на информационную безопасность.
A.14.1.3	Разработка и реализация планов обеспечения непрерывности, включающих информационную безопасность	Средство управления Должны быть разработаны и реализованы планы по обеспечению и восстановлению операций, которые гарантируют после остановки или сбоя критичных бизнес-процессов доступность информации на требуемом уровне и за требуемое время.
A.14.1.4	Структура планирования непрерывности бизнеса	Средство управления Должна поддерживаться единая структура планов обеспечения непрерывности бизнеса, чтобы гарантировать непротиворечивость всех планов, постоянный учет требований информационной безопасности и определение приоритетов для тестирования и сопровождения.
A.14.1.5	Тестирование, сопровождение и переоценка планов обеспечения непрерывности бизнеса	Средство управления Планы обеспечения непрерывности бизнеса должны регулярно тестироваться и обновляться, чтобы гарантировать их актуальность и эффективность.

A.15 Соответствие формальным требованиям

A.15.1 Соответствие правовым требованиям

Цель: Избежать нарушений законов, основанных на законе обязательств, регулятивных или договорных обязательств, а также всех требований безопасности.

A.15.1.1	Определение необходимой правовой базы	Средство управления Для каждой информационной системы и организации должны быть явно определены, документированы и поддерживаться в актуальном состоянии все требования закона, регулятивные и договорные требования, а также подход организации, используемый для удовлетворения этих требований.
A.15.1.2	Права на интеллектуальную собственность (IPR)	Средство управления Должны быть реализованы 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.
A.15.1.3	Защита записей организации	Средство управления Важные записи должны быть защищены от потери, уничтожения и подделки в соответствии с требованиями закона, регулятивными и договорными требованиями, а также бизнес-требованиями.
A.15.1.4	Защита данных и конфиденциальность персональной информации	Средство управления Защита данных и конфиденциальность должны быть обеспечены в соответствии с требованиями соответствующего законодательства, регулятивных положений, если применяется, положений договоров.
A.15.1.5	Предотвращение ненадлежащего использования средств обработки информации	Средство управления Пользователи не должны применять средства обработки информации для несанкционированных целей.

A.15.1.6	Регламентирование криптографических средств управления	Средство управления Криптографические средства управления должны использоваться согласно всем соответствующим соглашениям, законам и регулятивным положениям.
A.15.2 Соответствие политикам безопасности и стандартам, техническое соответствие Цель: Обеспечить соответствие систем принятым в организации политикам и стандартам безопасности.		
A.15.2.1	Соответствие политикам и стандартам безопасности	Средство управления Менеджеры должны гарантировать, что все процедуры безопасности в их сфере ответственности выполняются корректно, что обеспечивает соответствие политикам и стандартам безопасности.
A.15.2.2	Проверка технического соответствия	Средство управления Информационные системы должны регулярно проверяться на соответствие стандартам обеспечения безопасности.
A.15.3 Анализ аудита информационных систем Цель: Максимизировать эффективность процесса аудита и минимизировать воздействие, с одной стороны, процесса аудита на информационные системы, а с другой – информационных систем на процесс аудита.		
A.15.3.1	Средства управления аудитом информационных систем	Средство управления Требования аудита и деятельность, включающая проверки производственных систем, должны быть тщательно спланированы и согласованы, чтобы минимизировать риск сбоев в бизнес-процессах.
A.15.3.2	Защита средств аудита информационных систем	Средство управления Доступ к средствам аудита информационных систем должен быть защищенным, чтобы предотвратить любое возможное ненадлежащее использование или компрометацию.

Приложение Б
(справочное)
Принципы OECD и настоящий стандарт

Принципы, приведенные в документе OECD Guidelines for the Security of Information Systems and Networks [1], применяются ко всей политике и ко всем уровням функционирования, которые управляют безопасностью информационных систем и сетей. Настоящий стандарт предоставляет общую схему системы управления информационной безопасностью для реализации некоторых принципов OECD с помощью модели ПРОК и процессов, описанных в разделах **4**, **5**, **6**, **7** и **8**, как указано в Таблице Б.1.

Таблица Б.1. Принципы OECD и модель ПРОК

Принцип OECD	**Соответствующий процесс СУИБ и этап ПРОК**
Осведомленность (Awareness) Участники процесса должны быть осведомлены о необходимости защиты информационных систем и сетей, а также о том, что они могут сделать для повышения безопасности.	Эта деятельность является составной частью этапа **Реализация** (см. **4.2.2** и **5.2.2**).
Ответственность Все участники процесса несут ответственность за безопасность информационных систем и сетей.	Эта деятельность является составной частью этапа **Реализация** (см. **4.2.2** и **5.1**).
Реагирование Участники процесса должны действовать своевременно и согласованно, чтобы предотвращать, и выявлять инциденты безопасности, а также реагировать на них.	Частично соответствует мониторингу на этапе **Проверка** (см. **4.2.3** и **6–7.3**) и реагированию на этапе **Совершенствование** (см. **4.2.4** и **8.1–8.3**). Кроме того, может охватываться некоторыми аспектами этапов **Планирование** и **Проверка**.
Оценка рисков Участники процесса должны выполнять оценку рисков.	Эта деятельность является составной частью этапа **Планирование** (см. **4.2.1)**, а переоценка рисков является частью этапа **Проверка** (см. **4.2.3** и **6–7.3**).
Разработка и реализация безопасности Участники процесса должны включать безопасность в число важнейших элементов информационных систем и сетей.	По завершении оценки рисков выбираются средства управления для обработки рисков, что является составной частью этапа **Планирование** (см. **4.2.1**). Затем этап **Реализация** (см. **4.2.2** и **5.2**) охватывает реализацию и рабочую эксплуатацию этих средств управления.
Управление безопасностью Участники процесса должны принять комплексный подход к управлению безопасностью.	Управление рисками – это процесс, который включает в себя предотвращение, выявление и реагирование на инциденты, постоянное сопровождение, анализ и аудит. Все эти аспекты охвачены этапами **Планирование, Реализация, Проверка** и **Совершенствование**.
Переоценка Участники процесса должны пересматривать и переоценивать безопасность информационных систем и сетей, а также вносить необходимые изменения в политики, правила, критерии и процедуры безопасности.	Переоценка информационной безопасности является составной частью этапа **Проверка** (см. **4.2.3** и **6–7.3**), на котором должен проводиться регулярный анализ для проверки эффективности системы управления информационной безопасностью; повышение безопасности является составной частью этапа **Совершенствование** (см. **4.2.4** и **8.1–8.3**).

Приложение В
(справочное)
Соответствие между стандартами *СТ РК ИСО 9001-2001, СТ РК ГОСТ Р ИСО 14001-2000* и настоящим стандартом

В Таблице В.1 представлено соответствие между стандартами *СТ РК ИСО 9001-2001, СТ РК ГОСТ Р 14001-2000* и настоящим стандартом.

Таблица В.1. Соответствие между стандартами *СТ РК ИСО 9001-2001, СТ РК ГОСТ Р 14001-2000* и настоящим стандартом

Настоящий стандарт	**СТ РК ИСО 9001-2001**	**СТ РК ГОСТ Р ИСО 14001-2000**
Введение	**Введение**	**Введение**
Общие положения	Общие положения	
Процессный подход	Процессный подход	
	Связь со стандартом СТ РК ИСО 9004	
Совместимость с другими системами управления	Совместимость с другими системами менеджмента	
1 Область применения	**1 Область применения**	**1 Область применения**
1.1 Общие положения	1.1 Общие положения	
1.2 Применимость	1.2 Применимость	
2 Нормативные ссылки	**2 Нормативные ссылки**	**2 Нормативные ссылки**
3 Термины и определения	**3 Термины и определения**	**3 Термины и определения**
4 Система управления информационной безопасностью	**4 Система менеджмента качества**	**4 Требования к системе управления окружающей средой**
4.1 Общие требования	4.1 Общие требования	4.1 Общие требования
4.2 Разработка и управление СУИБ		
4.2.1 Разработка СУИБ		
4.2.2 Реализация и эксплуатация СУИБ		4.4 Реализация и эксплуатация
4.2.3 Мониторинг и анализ СУИБ	8.2.3 Мониторинг и измерение процессов	4.5.1 Мониторинг и измерение
	8.2.4 Мониторинг и измерение процессов продукта	
4.2.4 Сопровождение и совершенствование СУИБ		
4.3 Требования к документации	4.2 Требования к документации	
4.3.1 Общие требования	4.2.1 Общие требования	
	4.2.2 Руководство по качеству	
4.3.2 Управление документами	4.2.3 Управление документами	4.4.5 Управление документацией
4.3.3 Управление записями	4.2.4 Управление записями	4.5.4 Управление записями
5 Распределение обязанностей персонала	**5 Ответственность руководства**	

Настоящий стандарт	**СТ РК ИСО 9001-2001**	**СТ РК ГОСТ Р ИСО 14001-2000**
5.1 Приверженность руководства	5.1 Обязательства руководства 5.2 Ориентация на потребителя 5.3 Политика в области качества 5.4 Планирование 5.5 Ответственность, полномочия и обмен информацией	 4.2 Политика среды функционирования 4.3 Планирование
5.2 Управление ресурсами 5.2.1 Предоставление ресурсов 5.2.2 Обучение, осведомленность и компетентность	**6 Менеджмент ресурсов** 6.1 Обеспечение ресурсами 6.2 Человеческие ресурсы 6.2.2 Компетентность, осведомленность и подготовка 6.3 Инфраструктура 6.4 Производственная среда	 4.2.2 Компетентность, обучение и осведомленность
6 Внутренние аудиты СУИБ	8.2.2 Внутренние аудиты (проверки)	4.5.5 Внутренний аудит
7 Пересмотр СУИБ руководством 7.1 Общие положения 7.2 Исходные данные для анализа 7.3 Итоги анализа	5.6 Анализ со стороны руководства 5.6.1 Общие положения 5.6.2 Входные данные для анализа 5.6.3 Выходные данные анализа	4.6 Управление процедурой пересмотра некоторых положений
8 Совершенствование СУИБ 8.1 Постоянное совершенствование 8.2 Корректирующее воздействие 8.3 Превентивное воздействие	8.5 Измерение, анализ и улучшение 8.5.1 Постоянное совершенствование 8.5.3 Корректирующие воздействия 8.5.3 Предупреждающие действия	 4.5.3 Несоответствующее и корректирующее воздействие, превентивное воздействие
Приложение А Цели управления и средства управления (Annex A Control objectives and controls) **Приложение Б Принципы OECD и настоящий стандарт** **Приложение В Соответствие между стандартами СТ РК 9001:2001, ISO 14001:2004 и настоящим стандартом**	 **Приложение А Соответствие СТ РК ИСО 9001-2001 и СТ РК ГОСТ Р ИСО 14001-2000**	**Приложение А Руководство по использованию настоящего международного стандарта** **Приложение Б Соответствие между ISO 14001:2004 и ISO 9001:2000**

Приложение
(справочное)
Библиография

Публикации стандартов

[1] СТ РК ИСО 9001-2001, Система менеджмента качества. Требования

[2] ISO/IEC 13335-1:2004, Information technology— Security techniques— Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

[3] ISO/IEC TR 13335-3:1998, Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security

[4] ISO/IEC TR 13335-4:2000, Information technology— Guidelines for the management of IT Security — Part 4: Selection of safeguards

[5] СТ РК ГОСТ Р ИСО 14001-2000 Системы управления окружающей средой. Требования и руководство по применению

[6] ISO 14001:2004, Environmental management systems — Requirements with guidance for use

[7] ISO/IEC TR 18044:2004, Information technology— Security techniques— Information security incident management

[8] ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing

[9] ISO/IEC Guide 62:1996, General requirements for bodies operating assessment and certification/registration of quality systems

[10] ISO/IEC Guide 73:2002, Risk management— Vocabulary— Guidelines for use in standards

Другие публикации

[1] OECD, Guidelines for the Security of Information Systems and Networks— Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

[2] NIST SP 800-30, Risk Management Guide for Information Technology Systems

[3] Deming W.E., Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: информационная безопасность, система управления информационной безопасностью, СУИБ, оценка рисков, обработка рисков, политика информационной безопасности, цели управления, средства управления

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