ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Қазақстан Республикасының мемлекеттік техникалық реттеу жүйесі

Ақпаратты қорғау

АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІ ЖОБАЛАУҒА, ОРНАТУҒА, РЕТКЕ КЕЛТІРУГЕ, ПАЙДАЛАНУҒА ЖӘНЕ ОЛАРДЫҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУГЕ ҚОЙЫЛАТЫН ТАЛАПТАР

ҚР СТ 34.022-2006

Ресми басылым

Қазақстан Республикасының индустрия мен сауда министірлігі
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

Алғысөз

1 «Гранит» Арнаулы конструкторлық-технологиялық бюросы» ЖШС **ӘЗІРЛЕП ЕНГІЗДІ**

2 Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитет төрағасының 2006 жылғы 15 желтоқсандағы № 550 бұйрығымен **ҚАБЫЛДАНЫП ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 Осы стандартта мынадай халықаралық құжаттардың: «ИСО/МЭК 15408-1:2005 ұсынымдары. Ақпараттық технологиялар. Қорғау әдістері. Ақпараттық технологияларды қорғауды бағалау критерийлері. 1-бөлім. Кіріспе және жалпы үлгі. ИСО/МЭК 15408-2:2005 ұсынымдары. Ақпараттық технологиялар. Қорғау әдістері. Ақпараттық технологияларды қорғауды бағалауға арналған критерийлер. 2-бөлім. Қауіпсіздіктің пайдалану талаптары. ИСО/МЭК 15408-3:2005 ұсынымдары. Ақпараттық технологиялар. Қорғау әдістері. Ақпараттық технологияларды қорғауды бағалауға арналған критерийлер. 3-бөлім. Қорғауды қамтамасыз етуге қойылатын талаптар» құжаттарының негізгі нормативтік ережелері ескерілген

5 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ **2011 жыл**
ТЕКСЕРУ КЕЗЕҢДІЛІГІ **5 жыл**

6 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Қазақстан Республикасының мемлекеттік техникалық реттеу жүйесі

Ақпаратты қорғау

АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІ ЖОБАЛАУҒА, ОРНАТУҒА, РЕТКЕ КЕЛТІРУГЕ, ПАЙДАЛАНУҒА ЖӘНЕ ОЛАРДЫҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУГЕ ҚОЙЫЛАТЫН ТАЛАПТАР

Енгізілген күні 2008-01-01

1 Қолданылу саласы

Осы стандарт қызметтің барлық түрлерінде пайдаланылатын, құрылуы және қолданылуы процесінде мемлекеттік құпияларға [1] қатысты мәліметтер бар қорғалатын ақпаратты өңдеу жүзеге асырылатын ақпараттық жүйелерге таратылады.

Осы стандарт ақпараттық қауіпсіздік талаптарына жауап беретін ақпараттық жүйелерді әзірлеу, енгізу және пайдалану тәртібін белгілейді.

Осы стандарт ақпаратты қорғау сапасының кепілдігін жоғарлатуға үшін криптографиялық қорғау құралдарында қолданылады.

Осы стандарттың ережелерін ақпараттарды қорғау туралы құқықтық құжаттардың талаптарын орындау мәртебесі жөнінде міндеттемелер алған немесе міндетті Қазақстан Республикасының мемлекеттік органдары және ұйымдары қолдануға тиісті.

2 Нормативтік сілтемелер

Осы стандартта төмендегі нормативтік құжаттамаларға сілтемелер пайдаланылды:

ҚР СТ 34.005-2002 Ақпараттық технология. Негізгі терминдер мен анықтамалар.

ҚР СТ 34.013-2002 Ақпараттық технология. Ақпаратты есептегіш техника құралдарында өңдеу кезінде оны жанама электромагниттік сәулелену мен көздеулер арна бойынша жылыстауынан қорғау.

ҚР СТ 1171-2002 Қызметтік үй-жайларды акустикалық (сөйлеу) және дірілдету арналар бойынша акустикалық барлаудан қорғаудың тиімділігін бақылаудың типтік әдістемесі.

ҚР СТ 1200-2002 Ақпаратты қорғаудың мемлекеттік жүйесі. Мемлекеттік мекемелерде пайдаланылатын ақпаратты қорғаудың техникалық құралдары.

Ресми басылым

ҚР СТ 1201-2002 Ақпаратты қорғаудың мемлекеттік жүйесі. Ақпаратты қорғау құралдарын әзірлеу, келісу, бекіту және мемлекеттік тіркеуден өткізу тәртібі.

ҚР СТ 1202-2002 Ақпаратты қорғаудың мемлекеттік жүйесі. Ақпаратты қорғайтын техникалық құралдарға қойылатын жалпы талаптар.

ГОСТ 2.119-73 ҚҚБЖ. Нұсқалық жоба.

ГОСТ 2.120-73 ҚҚБЖ. Техникалық жоба.

ГОСТ 2.601-95 ҚҚБЖ. Пайдалану құжаттары.

ГОСТ 21552-84 Есептегіш техника құралдары. Жалпы техникалық талаптар, қабылдау, сынау әдістері, таңбалау, буып-түю, тасымалдау және сақтау.

ГОСТ 23773-88 Жалпы мақсатқа арналған есептегіш электрондық сандық машиналар. Сынау әдістері.

3 Терминдер мен анықтамалар

Осы стандартта ҚР СТ 34.005 стандартында белгіленген тиісті анықтамаларымен терминдер, сондай-ақ мынадай терминдер қолданылды:

3.1 **Тапсырыс беруші:** АЖ қойылатын талаптарды белгілейтін, оны құру жөніндегі жұмысты қаржыландыратын немесе оның тапсырысы бойынша АЖ құру (дамыту) және қызмет көрсету жүзеге асырылатын заңды тұлға (меншіктік тұлғасына тәуелсіз мемлекеттік орган немесе ұйым).

3.2 **Ақпараттық жүйе:** Ақпарат беретін және таратын, адами, техникалық және қаржылық ресурстар сияқты тиісті ұйымдастырушылық ресурстармен бірге ақпаратты өңдеу жүйесі.

3.3 **Мемлекеттік құпиялар:** Мемлекеттік және қызметтік құпияны құрайтын, таратылуына мемлекет тиімді әскери, экономикалық, ғылыми-техникалық, сыртқы экономикалық, барлау, контрбарлау, жедел іздестіру қызметтерін және өзге халықаралық құқықтың жалпы қабылданған нормаларына қайшы келмейтін қызметті жүзеге асыру мақсатында шек қоятын мемлекет қорғауындағы мәліметтер.

3.4 **Мемлекеттік құпия:** Жариялануы немесе жойылуы Қазақстан Республикасының ұлттық қауіпсіздігіне зиян келтіретін немесе зиян келтіруі мүмкін әскери, экономикалық, саяси және өзге сипаттағы мәліметтер.

3.5 **Қызметтік құпия:** Мемлекеттік құпия құрамына кіре алатын, жариялануы немесе жойылуы мемлекеттің ұлттық мүдделеріне, Қазақстан Республикасының мемлекеттік органдар мен ұйымдарының мүдделеріне зиян келтіруі мүмкін, жеке деректер сипаты бар мәліметтер.

3.6 **Қорғалатын ақпарат**: Жеке меншік болып табылатын және құқықтық құжаттар талаптарына немесе ақпарат иесі қойған талаптарға сәйкес қорғалуға тиісті ақпарат.

3.7 **Ақпараттандыру объектісі:** Берілген ақпараттық технологияға сәйкес пайдаланылатын ақпараттық ресурстардың, ақпаратты өңдеу құралдары мен жүйелерінің, ақпараттандыру объектісін қамтамасыз ететін құралдардың, олар орнатылған үй-жайлардың немесе объектілердің (ғимараттардың, құрылыстардың, техникалық құралдардың) немесе олар орнатылған үй-жайдың немесе объектінің жиынтығы.

3.8 **Ақпараттық қауіпсіздік:** АЖ ақпараты мен жабдығының құпиялыққа (санкцияланған қол жеткізуді қамтамасыз ету), бүтіндікке және қол жетімділікке қауіп төндіретін факторлардан қорғау.

3.9 **Қауіп-қатерлерді талдау:** АЖ қауіпсіздігіне және оның жеке құрамбөліктеріне төнетін қауіпті анықтау, олардың сипаттамаларын және әлуетті зиянын анықтау, сондай-ақ бақылаушы өлшегіш.

3.10 **Ақпарат қауіпсіздігіне қауіп-қатер:** Іске асырылуы ақпараттық процестерде заңды және жеке тұлғалардың құқықтарын, еркіндігі мен заңды мүдделерін бұзуға әкелетін ақпараттық қауіпсіздік объектілеріне қауіп төндіретін себептердің, шарттар мен факторлардың жиынтығы.

3.11 **Қорғалатын ақпаратқа әсер етуші фактор:** Нәтижесі қорғалатын ақпараттың таралуы, бұрмалануы, жойылуы немесе ақпаратқа қол жеткізуді бұғаттау болуы мүмкін құбылыс, әрекет немесе процесс.

3.12 **Ақпаратқа санкциясыз әсер ету**: Ақпараттың жария болуына, бұрмалауына, қолдан жасалуына, жойылуына, және оған қол жеткізілуін бұғаттауға, сондай-ақ ақпарат тасымалдаушының жойылып кетуіне, жойылуына немесе жаңылысуына әкелетін қол жеткізудің белгіленген құқықтарын және/немесе ережелерін бұза отырып қорғалатын ақпаратқа әсер ету.

3.13 **Ақпаратқа абайсызда әсер ету:** Ақпаратты пайдаланушының қателігі, техникалық және бағдарламалық құралдардың жаңылысуы, АЖ, сондай-ақ табиғи құбылыстар немесе техникалық құралдардың, жүйелердің жұмыс атқаруымен немесе ақпаратты бұрмалауға, жоюға, көшіруге, оған қол жеткізуді бұғаттауға, сондай-ақ оны тасымалдаушының жойылып кетуіне, жойылуына немесе жұмысының жаңылысуына әкелетін адам қызметімен байланысты өзге де ақпаратты өзгертуге мақсатқа сай бағытталған әсер.

3.14 **Ақпараттық қауіпсіздік саясаты:** Ақпараттық қауіпсіздік (АҚк) саласында басқару және жобалық шешімдерді анықтайтын құжаттар жиынтығы.

3.15 **Қорғау пішіні:** Атқарымдық талаптардың және кепілділік талаптарының терминдерімен ҚА қамтамасыз ету міндеттерін сипаттайтын құжат.

3.16 **ҚА қамтамасыз ету тетіктерінің кепілділігі:** ҚА қамтамасыз ететін пайдаланылатын тетіктерінің таңдалған атқарымдық талаптарға барабарлығын бағалау.

3.17 **Техникалық тапсырма:** Тапсырыс берушінің келісім-шартты жүзеге асыру кезінде орындалатын міндеттерді сипаттау және анықтау үшін құрал ретінде қолданылатын құжат.

3.18 **Пайдаланушы:** АЖ –ге командалар мен хабарламалар жіберетін және одан ақпарат алатын біреу немесе бір нәрсе. Машиналар немесе басқа жүйелер, сонымен қатар адамдар пайдаланушылар бола алады.

3.19 **АЖ әдістемелік қамтамасыз ету:** Автоматтандырылған қызметті, пайдаланушының нұсқаулықтарын орындау жүйесін және қосалқы жүйесін, әдістемесін (технологиясын) сипаттауды қоса, пайдаланушының ақпараттандыру құралдары жиынтығымен өзара әрекетін сипаттайтын құжаттар.

3.20 **АЖ ұйымдық қамтамасыз ету:** АЖ жұмыс жасау кезінде бөлімшелердің ұйымдық құрылымын, функцияларын және өзара әрекеттесу тәртібін, соның ішінде қызметкерлер нұсқаулықтарын белгілейтін құжаттар (ережелер, қызмет нұсқаулықтары, штаттық кестелер, біліктілік талаптары және т.б.).

3.21 **АЖ құрамбөлігі:** АЖ бөлімшесіндегі белгілі бір функцияны орындайтын және оның жұмысын қамтамасыз ететін қамтамасыз ету түрлерінің (техникалық, бағдарламалық, ақпараттық және басқа) бір элементі.

3.22 **Ақпараттық технологиялар жабдығы:** Деректерді және байланыс хабарламаларын енгізумен, сақтаумен, бейнелеумен, іздеумен, берумен, өңдеумен, басқарумен немесе жалғаумен байланысты функцияны орындайтын кез келген жабдық.

3.23 **Режимді үй-жайлар:** Құпия жұмыстар жасалатын, құпия құжаттар мен өнімдер сақталатын, басқа құпия ақпарат таралатын, сонымен қатар оны өңдеуге арналған техникалық құралдар орнатылған үй-жайлар.

3.24 **Негізгі техникалық құралдар:** Есептегіш техника құралдары, байланыс, дыбыс жазу мен дыбыс күшейту және дыбыс жаңғырту құралдары, сөйлесу және теледидар құрылғылары, құжаттарды дайындау мен көбейту құралдары, киножобалық аппаратура, электрожабдықтар жүйелері және құпия ақпаратты өңдеуге қолданылатын немесе құпия ақпаратты өңдеуге қолданылмайтын, бірақ режимді үй-жайлардағы басқа құралдар мен жүйелер.

3.25 **Көмекші техникалық құралдар**: Құпия ақпаратты өңдеуде тікелей қатысы жоқ, бірақ негізгі техникалық құралдармен бірге қолданылатын және негізгі техникалық құралдардың электромагниттік өріс аймағындағы техникалық құралдар.

4 Белгілер мен қысқартулар

Осы стандартта мынадай белгілер мен қысқартулар қолданылды:
ҚА - ақпараттық қауіпсіздік;
АЖ – ақпараттық жүйе;
АҚ – ақпаратты қорғау;
ТТТ – тактикалық-техникалық тапсырма;
ҒЗЖ – ғылыми-зерттеу жұмыс;
ТКЖ - тәжірибелік-құрастырылымдық жұмыс;
ЖЭМСШК - жанама электромагнитті сәулеленулер мен көздеулер;
ҚНмЕ – құрылыс нормалары мен ережелер.

5 Жалпы ережелер

5.1 АЖ құрудың және іске енгізудің мақсатқа сәйкестігі әлеуметтік, ғылыми-техникалық немесе АЖ жұмысқа енгізу нәтижесінде алынатын басқа тиімді әсерлермен анықталады.

5.2 АЖ жобалау (жаңғырту) және енгізу әдетте ТҚЖ шегінде жүргізіледі. ТКЖ негізгі қатысушыларының функциялары, олардың арасындағы өзара қарым-қатынастар және аяқталған ТКЖ іске асыру тәртібі ҚР СТ 1201 анықталған.

5.3 Жаңадан құрылатын (жаңғыртылатын) АЖ жобалау және енгізу ТТ сәйкес жүргізіледі. АЖ-дегі ТТ АЖ-ге қойылатын талаптарды, құру (жаңғырту) тәртібін және пайдалануға енгізу кезінде қабылдауды анықтайтын негізгі құжат болып табылады.

5.4 АЖ жобалау (жаңғырту), құрастыру және пайдалану процесінде АЖ техникалық, бағдарламалық құралдарына және ақпараттық ресурстарына әзірлеушілердің, құрастыру мен баптау жөніндегі мамандардың, пайдаланушылардың, қызмет көрсететін және пайдаланушы қызметкерлер құрамының қол жеткізуге рұқсат беру жүйесі ұйымдастырылуға тиіс. Мамандардың аталған топтарында тиісті нысаны бойынша мемлекеттік құпияларға қол жеткізуге рұқсаты болуға тиіс.

5.5 Әзірлеушілердің, пайдаланушылардың, қызмет көрсететін және пайдаланушы қызметкерлердің АЖ ресурстарына қол жеткізу жөніндегі өкілеттіктерін тапсырыс беруші белгілейді.

5.6 АЖ тапсырыс берушісі, меншік иесі (иесі), сонымен қатар АЖ құруға қатысушы-ұйымдар АЖ-де өңделетін ақпаратты қорғауды қамтамасыз етуге және АЖ құрудың және пайдаланудың барлық сатыларында АҚ бойынша жұмыстарды орындауға жауап береді.

5.7 АЖ құру жөніндегі жұмыстарға қатысушы ұйымдарда ақпаратты қорғау саласында жұмыс жасау құқығына лицензиясы болуға тиіс. Ұйымдарды лицензиялау белгіленген тәртіппен [1] жүзеге асырылады.

5.8 АЖ құру үшін ақпаратты өңдейтін сериялық шығарылатын да, сондай-ақ жаңадан әзірленген техникалық және бағдарламалық құралдарда, сонымен қатар ақпаратты қорғайтын техникалық, бағдарламалық, бағдарламалық-техникалық, криптографиялық құралдар және АҚ тиімділігін бақылауға арналған құралдар қолданыла алады. Қолданылатын құралдарда сәйкестікті растау жөніндегі тиісті органдар берген ақпарат қауіпсіздігі талаптары бойынша сәйкестік сертификаттары болуға тиіс.

Жаңадан әзірленген құралдар АЖ тәжірибелік пайдалану басталғанға дейін белгілі тәртіппен сертификатталуға тиіс.

5.9 АЖ пайдалануды тоқтату мынадай негіздер бойынша:

- белгіленген тәртіппен рәсімделген АЖ меншік иесінің (иесінің) шешімі бойынша;
- қорғалатын ақпараттың ақпаратты қорғау жөніндегі нормативтік құжаттардың талабына сәйкес еместігі себебінен немесе ақпараттың жылыстауына әкелетін себептерден немесе басқа қауіп-қатерлерден қадағалау (бақылау) органы қабылдаған шешімге байланысты;
- сот шешімі бойынша қарастырылады.

6 Ақпараттық жүйелерді жобалау

6.1 АЖ құру сатылары мен кезеңдері

АЖ құру процесі бір мезгілге реттелген, өзара байланысты, сатылар мен кезеңдерге біріккен жұмыстардың жиынтығын білдіреді. АЖ құру сатылары мен кезеңдері 1-кестеде берілген.

1 кесте - АЖ құру сатылары мен кезеңдері

АЖ құру саты	Жұмыс кезеңдері
1 АЖ-ге қойылатын талаптарды қалыптастыру	1.1 Нысанды тексеру және АЖ құру қажеттілігін негіздеу. 1.2 АЖ-ге тапсырыс берушінің бастапқы талаптарын қалыптастыру. 1.3 Орындалатын жұмыс туралы есепті және АЖ әзірлеуге өтінімдерді рәсімдеу.
2 АЖ тұжырымдамасын және ҚА тұжырымдамасын әзірлеу	2.1 Ақпараттандыру нысанын зерттеу. 2.2 ҒЗЖ жүргізу (қажет кезде). 2.3 АЖ тұжырымдамасының нұсқалары мен ҚА тұжырымдамасының нұсқаларын әзірлеу, АЖ тұжырымдамасының нұсқалары мен ҚА тұжырымдамасының нұсқаларын таңдау.

	2.4 Аванжобаға техникалық (тактика-техникалық) тапсырма әзірлеу. 2.5 Орындалған жұмыс туралы есепті рәсімдеу. 2.6 Аванжоба әзірлеуге тапсырыс беруші мен орындаушының ортақ шешімін рәсімдеу.
3 Аванжоба	3.1 АЖ тұтастай ТТ-да әзірлеу. 3.2 АЖ ішкі жүйелеріне жеке ТТ әзірлеу.
4 Эскиз жоба	4.1 Жұмыс жасау тетіктерін іске асыратын АЖ таңдалған нұсқасы бойынша алдын ала жобалық шешімдерді әзірлеу. 4.2 АЖ және оның бөлімдеріне құжаттама әзірлеу.
5 Техникалық жоба	5.1 Жүйе бойынша және оның құрамбөліктеріне жобалық шешімдерді әзірлеу. 5.2 АЖ-ге және оның бөліктеріне құжаттама әзірлеу. 5.3 Жинақтаушы бұйымға арналған құжаттарды және/немесе оларды әзірлеуге арналған техникалық тапсырмаларды (техникалық талаптарды) әзірлеу және рәсімдеу. 5.4 Ақпараттандыру объектісі жобасының аралық бөліктеріне жобалауға тапсырмалар әзірлеу.
6 Жұмыс құжаттамасы	6.1 АЖ-ге және оның құрамбөліктеріне жұмыс құжаттамасын әзірлеу. 6.2 Бағдарламаларды әзірлеу немесе бейімдеу.
7 Қолданысқа енгізу	7.1 Ақпараттандыру объектісін АЖ қолданысқа енгізуіне дайындау. 7.2 Қызметкерлерді дайындау. 7.3 АЖ жеткізіліп берілетін бұйымдармен толықтыру. 7.4 Құрылыстық-жинақтау жұмыстары. 7.5 Іске қосу-баптау жұмыстары. 7.6 Алдын ала сынақтарды өткізу. 7.7 Тәжірибелік пайдалануды өткізу. 7.8 Қабылдау сынақтарын өткізу.
8 АЖ пайдалану	8.1 Кепілді міндеттемелерге сәйкес жұмыстарды орындау. 8.2 АЖ пайдалану.

6.1.1 АЖ құру (дамыту) кезінде орындалатын жұмыстардың сатылары мен кезеңдерінің құрамы, реттілігі мен іске асырылу мерзімдері осы

стандартта берілген жұмыстардың сатылары мен кезеңдерінің қатарынан жүйе құру (дамыту) үшін техникалық тапсырмада (немесе келісім-шартты орындау ведомосында) белгіленеді.

6.1.2 Құрылатын АЖ ерекшелігіне және оны құру жағдайларына байланысты жұмыстардың жеке кезеңдерін алдыңғы сатылар аяқталғанға дейін орындау және жұмыстар кезеңдерін уақытпен параллель орындауға рұқсат етіледі.

6.1.3 АЖ әзірлеуге арналған техникалық тапсырма және жобалық-сметалық құжаттама міндетті түрде мемлекеттік құпияларды және ақпараттық қауіпсіздікті қорғау жөніндегі уәкілетті мемлекеттік органмен, ақпарат және байланыс және ұлттық қауіпсіздігін қамтамасыз ету саласындағы уәкілетті органдармен келісіп шешіледі.

6.2 Жобалау кезеңдері бойынша жұмыстардың мазмұны

6.2.1 1.1 «Объектіні тексеру және АЖ құру қажеттігін негіздеу» кезеңінде жалпы жағдайда мынадай:

- ақпараттандыру объектісін тексеру (мәліметтерді жинау және талдау), ақпараттық қауіпсіздік (АҚк) режимі жағдайын бағалау;
- жобаланатын АЖ функциялары мен міндеттерін іске асыру кезінде ҚА режимін қамтамасыз ету жөніндегі талаптарды қалыптастыру;
- шетелдік және отандық аналогтар туралы мәліметтер жинау;
- АЖ құрудың мақсатқа сәйкестілігінің техникалық-экономикалық, әлеуметтік және т.с.с бағалау жұмыстарын орындау қарастырылады.

6.2.2 АЖ-ге 1.2 «Тапсырыс берушінің бастапқы талаптарын қалыптастыру» кезеңінде АЖ-ге қойылатын талаптарды қалыптастыру үшін бастапқы деректерді:

- ақпараттандыру объектісінің сипаттамасын;
- құрылатын АЖ функциялары мен міндеттерін;
- АЖ (климаттық және механикалық әрекеттерге қойылатын талаптар) жұмыс жасау шарттарын;
- АЖ әр функциясы мен міндеті бойынша (қол жетімсіздік мерзімі, қол жеткізу уақыты және заттық саламен анықталатын басқа көрсеткіштер; сенімділік, сақтау, жеткізу көрсеткіштері; ақпараттың құпиялығының үдеуі) ҚА режимін қамтамасыз етуге қойылатын талаптарды;
- АЖ құру және пайдалану шарттарын;
- әзірлеуге кететін рұқсат етілетін шығындарды шектеуді;
- ҒЗЖ өткізуді (қажет кезде);
- АЖ қойылатын талаптарды қалыптастыруды және ресімдеуді дайындау жүргізіледі.

6.2.3 1.3 «Орындалған жұмыс туралы есепті және АЖ әзірлеуге берілген өтініштерді рәсімдеу» кезеңінде осы кезеңде орындалған жұмыстар туралы

есепті рәсімдеу жүргізіледі және АЖ әзірлеуге өтініш немесе басқа оның орнына жүретін құжат ресімделеді.

6.2.4 2.1 «Ақпараттандыру нысанын зерттеу» және 2.2 «ҒЗЖ жүргізу» кезеңдерінде ҒЗЖ орындаушы-ұйым ақпараттандыру объектісін егжей-тегжейлі зерттейді және тапсырыс берушінің талаптарын іске асыру мүмкіндігі жолдарын және бағалауды іздестірумен байланысты қажетті ҒЗЖ өткізеді, өткізілген ҒЗЖ бойынша есептерді рәсімдейді және бекітеді.

6.2.5 2.3 «Тапсырыс берушінің талаптарын қанағаттандыратын АЖ тұжырымдамасының және ҚА тұжырымдамасының нұсқаларын әзірлеу және АЖ тұжырымдамасының нұсқасы мен ҚА тұжырымдамасының нұсқасын таңдау» кезеңінде:

– құқықтық және келісім-шарттық талаптарды талдау;

– АЖ тұжырымдамасының балама нұсқаларын, ҚА тұжырымдамаларының балама нұсқаларын және оларды жүзеге асыру жоспарларын әзірлеу;

– жүйенің ақпараттық ресурстарлары душар етілуі мүмкін қауіп-қатерлерді (қауіптер топтарын) талдау;

– балама нұсқаларды жүзеге асыруға қажетті ресурстарды бағалау және жұмыс жасауды қамтамасыз ету;

– нұсқалардың ерекшелігін және кемшілігін бағалау;

– тапсырыс берушінің талаптарын және АЖ жорамалданған нұсқасының сипаттамаларын салыстыру;

– АЖ тұжырымдамасының оңтайлы нұсқасын таңдау және ҚА тұжырымдамасының оңтайлы нұсқасын таңдау;

– АЖ сапасын бағалау тәртібін және қабылдау шарттарын анықтау;

– АЖ-ден алынатын әсерлерді бағалау жүргізіледі.

6.2.6 2.4 «Аванжобаға арналған техникалық (тактикалық - техникалық) тапсырма әзірлеу» кезеңінде аванжобаға ТТ (ТТТ) әзірлеу, келісу мен бекіту және, қажетіне қарай, АЖ құрама бөліктеріне техникалық тапсырмалар жүргізіледі.

6.2.7 2.5 «Орындалған жұмыс туралы есеп рәсімдеу» кезеңінде сатылардағы орындалған жұмыстардың сипаттамасы бар есеп және АЖ тұжырымдамасының ұсынылған нұсқасының және ҚА тұжырымдамасының ұсынылған нұсқасының сипаттамасы мен негіздемесі дайындалады және ресімделеді.

6.2.8 2.6 «Аванжоба әзірлеуге тапсырыс беруші мен орындаушының ортақ шешімін дайындау» кезеңінде келісім-шарт жасалады немесе тапсырма беруші мен орындаушының аванжоба әзірлеуге арналған ортақ шешімі ресімделеді.

6.2.9 3.1 «АЖ-ге ТТ әзірлеу» кезеңі және 3.2 «АЖ қосалқы жүйелеріне жеке ТТ әзірлеу» кезеңі 6.2.9.1 – 6.2.9.8 жұмыстарын орындауды қарастырады.

6.2.9.1 АЖ құрудың мақсатқа сәйкестілігінің техникалық негіздемесі, оны қолдану мәселелерін түбегейлі қарастыру.

6.2.9.2 АЖ техникалық мүмкіндіктерін, құру жолдарын анықтау, техникалық шешімдердің мүмкін нұсқаларын қарастыру, АЖ оңтайлы нұсқасы мен құрамын таңдаудың негіздемесі.

6.2.9.3 АЖ қойылатын талаптарды қалыптастыру:

– жалпы техникалық талаптар;
– АЖ функцияларына қойылатын талаптар;
– техникалық қамтамасыз етуге қойылатын талаптар;
– бағдарламалық қамтамасыз етуге қойылатын талаптар;
– ақпараттық қамтамасыз етуге қойылатын талаптар;
– лингвистикалық қамтамасыз етуге қойылатын талаптар;
– ұйымдық қамтамасыз етуге қойылатын талаптар;
– методикалық қамтамасыз етуге қойылатын талаптар;
– ақпараттық қауіп-қатерлердің сипаттамасы;
– АЖ-де ақпаратты қорғау міндеттері;
– қорғалатын ақпараттың тізімі және оны қорғау тиімділігінің талап етілетін нормалары (деңгейлері);
– өздері үшін қауіп-қатерді талдау жүргізілетін жүйе элементтерін таңдау;
– қорғау пішіні және АҚ құралдарына қойылатын талаптар;
– ҚА режимін қамтамасыз етуге қойылатын талаптар;
– ұйымның үздіксіз жұмыс істеуін қамтамасыз ету жөніндегі талаптар;
– қызметкерлер құрамының даярлығына қойылатын талаптар;
– құқықтық қамтамасыз етуге қойылатын талаптар;
– құжаттамаға қойылатын талаптар.

6.2.9.4 Жобаланатын АЖ-ні тапсырма берушімен келісілген көрсеткіштер бойынша ұқсас отандық және шетелдік үлгілермен салыстыру.

6.2.9.5 Сынақтар жасау үшін АЖ құрамбөліктерінің үлгілерін анықтау.

6.2.9.6 ТКЖ орындаудың лимиттік құнын және АЖ пайдалануға шамамен алынған шығындарды есептеу.

6.2.9.7 АЖ құру бойынша ТКЖ-ға ТТ әзірлеу.

6.2.9.8 Аванжоба орындау қорытынды бойынша есеп құжаттаманы сол бойынша қабылданған шешімдерді негіздей отырып жасау.

6.2.10 «Эскиз жоба» сатысы ТКЖ эскиз жобасын әзірлеу кезеңінде 4.1 және 4.2 жұмыстарының сатыларын орындауды қарастырады.

6.2.10.1 4.1 «Жұмыс жасау тетіктерін іске асыратын АЖ таңдалған нұсқасы бойынша алдын ала жобалық шешімдерді әзірлеу» кезеңінде мыналар:

– АЖ функциялары;
– қосалқы жүйелердің функциялары, олардың мақсаттары мен әсерлері;

– міндеттер жиынтығының және жеке міндеттердің құрамы;

– ақпараттық ресурстардың тұжырымдамасы, оның ұлғайтылған құрылымы;

– дерекқорды басқару жүйесінің функциялары және есептегіш жүйенің құрамы;

– негізгі бағдарламалық құралдардың функциялары мен параметрлері;

– ҚА тәртібін қамтамасыз ететін жүйенің және қосалқы жүйенің құрылымы жөніндегі техникалық шешімдер, иерархия деңгейлері және ҚА басқару жүйе;

– ҚА режимін қамтамасыз ететін жүйенің жұмыс жасау режимдері мен оның жай-күйін диагностикалау жөніндегі техникалық шешімдер;

– жүйе сапасын сипаттайтын, ҚА режимін қамтамасыз ететін көрсеткіштердің сипаттамасы және оны өлшеу әдістері;

– ұсынылатын жоба шегінде қорғау қамтамасыз етілетін ҚА қауіп-қатерлерінің тізімі анықталады.

6.2.10.2 4.2 «АЖ-ге және оның бөлімдеріне арналған құжаттама әзірлеу» кезеңінде қабылданған шешімдердің толық жиынтығын сипаттау үшін қажетті және АЖ құру бойынша жұмыстарды онан әрі орындау үшін жеткілікті көлемде құжаттаманы әзірлеу, рәсімдеу, келісу және бекіту жүргізіледі.

Түсіндірме жазбада іске қосу, қалыпты және апаттық режимдерде ақпараттық жүйенің және АҚ техникалық құралдардың жұмыс жасауын және ҚА режимін қамтамасыз ететін техникалық құралдарды таңдауға негіздеме жүргізіледі.

6.2.11 «Техникалық жоба» сатысы ТКЖ техникалық жоба әзірлеу кезеңінде іске асырылады және оған 5.1 – 5.4 кезеңдері кіреді.

6.2.11.1 5.1 «Жүйе және оның құрамбөліктері бойынша жобалық шешімдерді әзірлеу» кезеңінде АЖ және оның бөліктері, жүйенің атқарымдық-алгоритмдік құрылымы бойынша, қызметкерлердің функциялары мен ұйымдастыру құрылымы бойынша, техникалық құралдар құрылымы бойынша, есеп шығару алгоритмдері мен қолданылатын тілдері бойынша, ақпараттық ресурстарды ұйымдастыру мен жүргізу бойынша, бағдарламалық қамтамасыз ету бойынша, деректерді жинауды және беруді ұйымдастыру бойынша жалпы шешімдерді әзірлеуді қамтамасыз етеді.

6.2.11.2 5.2 «АЖ-ге және оның бөлімдеріне құжаттама әзірлеу» кезеңінде жалпы жүйелік мәселелер бойынша, соның ішінде АЖ құрылымы бойынша және қамтамасыз ету түрлері бойынша соңғы шешімдер әзірленеді.

Кезеңде ҚА бөлігінде:

– үй-жайға кіру және жабдыққа қол жеткізу рұқсаты мәселелерін, ақпаратты тасымалдаушылармен жұмыс істеуді, ақпаратқа қол жеткізуді регламенттейтін қызметкерлердің лауазымдық нұсқаулары;

– АЖ-дегі әкімгерлік ережелер;

– АЖ-де пайдаланушылар жұмысының ережелері;

– басқа жақтың ұйымдарымен жұмыс жасау ережелері әзірленуге тиіс.

Қорғаудың кешендік жүйесінің негізгі құрайтын іс-шараларын қарай отырып, ҚА режимін қамтамасыз ету жөніндегі іс-шаралардың жоспары:

– қызметкерлердің жұмысын ұйымдастыру;

– ҚА физикалық қорғау және режимін сақтауды бақылау;

– бірнеше рет пайдалану жүйесінде қол жеткізуді ұйымдастыру;

– желілерде жұмысқа қабілеттікті демеу және ҚА қамтамасыз ету;

– қалпына келтіру жұмыстарын жоспарлау әзірленуге тиіс.

Жұмыс нәтижелері «Ақпаратты қорғау құралдары және қорғау тиімділігін бақылау құралдары» техникалық жобасында АЖ техникалық жобасының бөлімі сияқты жазылуға тиіс.

6.2.11.3 5.3 «Жинақтаушы бұйымдарға арналған құжаттарды және/немесе оларды әзірлеуге арналған техникалық тапсырмаларды (техникалық талаптарды) әзірлеу және рәсімдеу» кезеңінде:

– АЖ жинақтау үшін бұйымдарды жеткізуге арналған құжаттаманы дайындау және рәсімдеу;

– техникалық талаптар анықтау және сериялы жеткізілмейтін өнімдерді әзірлеуге ТТ құрастыру;

– ақпаратты қорғау құралдарына техникалық тапсырма әзірлеу және тәжірибелік үлгілер даярлау;

– ақпаратты қорғау тиімділігін бақылау құралдарына техникалық тапсырмалар әзірлеу және тәжірибелік үлгілер даярлау жүргізіледі.

6.2.11.4 5.4 «Ақпараттандыру объектісі жобасының аралық бөлімдерінде жобалауға тапсырмалар әзірлеу» кезеңінде, құрылыс, электротехникалық, коммуникациялық, санитарлық-техникалық және АЖ құрумен байланысты басқа дайындық жұмыстарын өткізу үшін АЖ жобасының аралық бөліктерінде жоба жасауға тапсырмаларды әзірлеу, рәсімдеу, келісу және бекіту жүзеге асырылады.

6.2.12 6.1 «АЖ-ге және оның құрамбөліктеріне жұмыс құжаттамасын әзірлеу» кезеңінде АЖ қолданысқа енгізу және оны пайдалану жөніндегі жұмыстарды орындауды қамтамасыз ету үшін, сонымен қатар жүйенің пайдалану сипаттамаларының деңгейін қабылданған жобалық шешімдерге сәйкес қолдау үшін барлық қажетті және жеткілікті мәліметтер, оны дайындау, келісу және бекіту бар жұмыс құжаттамасын әзірлеу жүргізіледі.

Мынадай:

– қызметкерлер жұмысын ұйымдастыру;

– АЖ физикалық қорғау және АҚ сақтауды бақылау;

– бірнеше рет пайдалану жүйесінде қол жеткізуді ұйымдастыру;

– жұмысқа қабілеттікті қолдау және желілерде АҚ қамтамасыз ету;

– қалпына келтіру жұмыстарын жоспарлау бөлімдері бар АҚ режимін қамтамасыз ету жөніндегі іс-шаралар жоспары әзірленуге тиіс.

Мыналар:

– үй-жайға кіру және жабдыққа қол жеткізу рұқсаты мәселелерін, ақпаратты тасымалдаушылармен жұмыс істеуді, ақпаратқа қол жеткізуді регламенттейтін қызметкерлердің лауазымдық нұсқаулары;

– АЖ-дегі әкімгерлік ережелер;

– АЖ-де пайдаланушылар жұмысының ережелері;

– басқа жақтың ұйымдарымен жұмыс жасау ережелері әзірленуге тиіс.

Сонымен қатар осы кезеңде АЖ-ге нақтылы ТКЖ шегінде ТТ бойынша даярланған құрамбөліктердің тәжірибелік үлгілері даярлануға тиіс және олар сынақтардан өткізілуге тиіс.

6.2 «Бағдарламаны әзірлеу немесе бейімдеу» кезеңінде жүйенің бағдарламалары мен бағдарламалық құралдарының әзірленуі, сатып алынатын құралдарды таңдау, бейімдеу және/немесе байластыру, сәйкестікті растау жөніндегі аккредиттелген органдар жүргізген сатып алынған бағдарламалық құралдардың ақпарат қауіпсіздігі бойынша белгіленген талаптарға сәйкестігін растау жүргізіледі.

Деректерді жинауды және беруді ұйымдастыру жөніндегі техникалық шешімдер, сонымен қатар АҚ режиміне қатысты бағдарламалық қамтамасыз ету жөніндегі техникалық шешімдер берілуге тиіс.

6.2.13 7.1 «Ақпараттандыру объектісін АЖ қолданысқа енгізуге дайындау» кезеңінде ақпараттандыру объектісін АЖ қолданысқа енгізуге ұйымдастырушылық даярлау бойынша жұмыстар, соның ішінде:

– АЖ ұйқастыру құрылымы бойынша жобалық шешімдерді іске асыру;

– бөлімшелерді нұсқаулық-әдістемелік мәліметтермен қамтамасыз ету;

– ақпарат жіктеуіштерін енгізу;

– АЖ-де АҚ анықтайтын сыни маңызды функциялар мен жүйелерді табу;

– АҚ үшін болуы мүмкін апаттар тізімін және олардың салдарын анықтау;

– стихиялық апаттардан, апаттардан, бұзушыларды шабуылдарынан болған, жұмыстағы бұзылу нәтижелерін жоюға бағытталған АҚ шараларын әзірлеу жүргізіледі.

Бірнеше рет пайдалану жүйесінде сондай-ақ АЖ қол жеткізу мәселелері шешілуге тиіс:

– пайдаланушыларды тіркеу;

– пайдаланушылардың құпия сөздерін басқару;

– артықшылықтарды басқару;

– пайдаланушылардың қол жеткізу құқықтарын қайта қарау;

– жүйені, соның ішінде ҚА жүйесін әкімшілік ету үшін айрықша қол жеткізуді басқару.

Пайдалануға дайындау процесінде ақпараттандыру объектісін физикалық қорғау ұйымдастырылуға және мынадай:

– үй-жайға кіру рұқсаты;

– құпиялылықты сақтау;

– оқиғаларды тіркеу журналдарын жүргізу – АЖ–ге қол жеткізуге (сәтті және сәтсіз) ұмтылуды есепке алу;

– ақпарат тасымалдаушыларына және оларды қорғауға (пайдаланушыларды тіркеу, артықшылықтарды басқару; пайдаланушының құпия сөздерін басқару; пайдаланушылардың қол жеткізу құқықтарын қайта қарау; терминалдардың тұрып қалған уақытын қадағалау және бақылаусыз қалған пайдаланушы жабдығын қорғау; қызмет көрсетулерге қол жеткізуді шектеу; қосудың рұқсат етілген кезеңін шектеу) қол жеткізуді ұйымдастыру;

– АЖ бойынша құжаттамаларға қол жеткізу мәселелер бөлігінде ҚА режимін сақтауға бақылау жасауды ұйымдастырылуға тиіс.

7.2 «Қызметкерлерді дайындау» кезеңінде қызметкерлерді оқыту және олардың АЖ жұмысын қамтамасыз етуге даярлығына тексеру жүргізіледі, сондай-ақ АЖ-дегі жұмысқа пайдаланушылардың қол жеткізу, ҚА физикалық қорғауды және оның режимін сақтауға бақылауды ұйымдастыру мәселелері шешілуге тиіс.

7.3 «АЖ жеткізіліп берілетін бұйымдармен толықтыру» кезеңінде сериялық және жеке өндірістің жинақтаушы өнімдерін, материалдар мен монтаждау бұйымдарын алу қамтамасыз етіледі. Олардың сапасын кіріс бақылау және ақпараттық қауіпсіздіктің белгіленген талаптарына сәйкестігін растау жүргізіледі.

7.4 «Құрылыс-монтаж жұмыстары» кезеңінде:

– арнайы үй-жайлардың (ғимараттардың, құрылыстардың) құрылысы бойынша АЖ техникалық құралдары мен қызметкерлерін орналастыру үшін жұмыстар орындау;

– кабельді арналарды құрастырып салу;

– техникалық құралдарын және байланыс жолдарын құрастыру бойынша жұмыстар орындау;

– құрастырылған техникалық құралдарды сынау;

– іске қосу-баптау жұмыстарын жүргізу үшін құрастырылған техникалық құралдарды беру жүргізіледі.

7.5 «Іске қосу-баптау жұмыстары» кезеңінде техникалық және бағдарламалық құралдарды автоном жөндеу, дерекқорға ақпарат енгізу және оны жүргізілу жүйесін тексеру, жүйенің барлық құралдарын құрама баптау жүргізіледі. Жұмыс жүргізу процесінде:

– үй-жайға кіруге рұқсат;

– құпиялылықты сақтау;

– оқиғаларды тіркеу журналдарын жүргізу;

– ақпарат тасымалдаушыларға қол жеткізуді ұйымдастыру;

– АЖ бойынша құжаттамаларға қол жеткізуді бақылау ұйымдастырылуға тиіс.

Іске қосу-баптау жұмыстары құпия емес (шартты) ақпаратты қолдану арқылы жүргізілуге тиіс.

7.6 «Алдын ала сынақтар жасау» кезеңінде:

– АЖ жұмысқа қабілеттілікке және алғашқы сынау бағдарламасы мен әдістемесі бойынша техникалық тапсырмаға сәйкестікке сынау;

– төтенше жағдайларға АЖ әрекет етуді тексеру және апаттық жұмыс режиміне өту;

– функцияларды орындау және бақылау міндеттерін шешу кезінде АЖ жұмыс жасайтын барлық режимдерінде ҚА бағдарламалық-техникалық тетіктерін тексеру;

– бұзылуды жою және АЖ арналған құрастырылымдық құжаттамаға өзгерістер енгізу;

– тәжірибелік пайдалануға АЖ қабылдау туралы сынау хаттамаларын және актіні рәсімдеу жүзеге асырылады.

7.7 «Тәжірибелік пайдалануды жүргізу» кезеңінде:

– АЖ тәжірибелік пайдалану;

– тәжірибелік пайдалану нәтижелерін талдау;

– АЖ бағдарламалық қамтамасыз етуді (қажет жағдайда), ақпаратты қорғау құралдарын және ақпаратты қорғау тиімділігін бақылау құралдарын түзету;

– жұмыстың барлық режимдерінде АЖ апаттық режимдерін қоса, АҚ техникалық құралдарын кешенді жөндеу;

– АЖ тәжірибелік пайдаландыру аяқталғаны туралы актіні рәсімдеу жүргізіледі.

7.8 «Қабылдау сынақтарын жүргізу» кезеңінде:

– Белгіленген тәртіппен бекітілген қабылдау сынақтарының бағдарламасы мен әдістемесіне сәйкес ТТ сәйкестігіне сынақтар жүргізу;

– сынау нәтижелерін талдау және сынау процесінде табылған кемшіліктерді жою;

– сынау хаттамаларын және АЖ пайдалануға қабылдау туралы актіні рәсімдеу;

– бюджеттік бағдарлама әкімгерінің әзірлеген АЖ-сін заңнамада белгіленген тәртіппен қабылдау;

– нормативтік құқықтық актілерге сәйкес ақпараттандыру және байланыс саласында уәкілетті орган жасаған АЖ салалық бағалау жүргізіледі.

АЖ пайдалануға енгізу күні деп қабылдау комиссиясының АЖ қолданысқа енгізу туралы актіге қол қойған күні саналады.

Қорғалатын ақпаратты өңдеу үшін АЖ қолдану сәйкестікті растау жөніндегі тиісті аккредиттелген орган жасаған ақпарат қауіпсіздігінің белгіленген талаптарына оның сәйкестігін растағаннан кейін ғана рұқсат етіледі.

АЖ қолдану мүмкіндігі туралы шешімді жүйенің қабылдау сынақтарын жүргізу жөніндегі комиссияның актісі негізінде тапсырыс беруші қабылдайды.

6.2.14 8.1 «Кепілді міндеттемелерге сәйкес жұмыстарды орындау» кезеңінде белгілеген кепілді мерзім ішінде АЖ пайдалану кезінде табылған кемшіліктерді жою, АЖ құжаттамаларына қажетті өзгертулер енгізу жөніндегі жұмыстар жүзеге асырылады.

8.2 «АЖ пайдалану» кезеңінде:

– АЖ жұмыс жасауын талдау;

– Нақты пайдалану сипаттамаларының жобалық мәндерден ауытқуларын табу және осы ауытқулардың себептерін белгілеу;

– табылған кемшіліктерді жою және пайдалану сипаттамаларының тұрақтығын және ҚА қамтамасыз ету;

– енгізілген өзгертулерді олар қатысты тұлғаларға жеткізетін белгіленген процедуралар мен ережелерге сәйкес құрастырылымдық құжаттамаға өзгертулер енгізу. бойынша жұмыстар жүзеге асырылады.

6.3 Сатылар бойынша жұмыстарды орындау нәтижелері

6.3.1 «АЖ қойылатын талаптарды қалыптастыру» сатысын орындау нәтижесі ғылыми-техникалық есеп, аванжобаға арналған техникалық тапсырма, АЖ құру үшін техникалық-экономикалық негіздеме мен тапсырыс болып табылады.

6.3.2 «АЖ тұжырымдамасын және ҚА тұжырымдамасын әзірлеу» сатысын орындау нәтижесі есеп беру болып табылады. Осы сатысында әзірленетін есепте, «Құрылатын АЖ функциялары мен міндеттері» бөлімінде «ҚА режимін қамтамасыз етуге қойылатын талаптар» қосалқы бөлімі болуға тиіс. Оның ішінде ҚА режимін АЖ әр функциясы мен міндеті бойынша қамтамасыз етуге қойылатын талаптар сипатталуға тиіс.

Құрылатын АЖ тұжырымдамасының нұсқасын таңдағаннан кейін мынадай:

– құқықтық және келісім-шарттық талаптар;

– АЖ функциялары мен міндеттері бойынша ҚА режимін қамтамасыз етуге қойылатын талаптар факторлары топтарын талдау негізінде АҚ тұжырымдамасы әзірленуге тиіс.

Талдау нәтижелері бойынша ұйымды тұтасымен:

– ҚА саласындағы ұйым көздейтін мақсаттар мен басымдылықтарды;

– осы мақсаттарға қол жеткізудегі жалпы бағыттарды;

– ұйым деңгейінде толығынан шешілуге тиіс ҚА бағдарламасының аспектілерін;

– лауазымды тұлғаларды және олардың ҚА бағдарламасын іске асыру бойынша міндеттерін қозғайтын ҚА негізгі ережелері қалыптастырылады.

ҚА саясатының тұжырымдамасы есеп түрінде ресімделуге тиіс.

6.3.3 «Аванжоба» сатысын орындау нәтижесі АЖ құруға арналған техникалық тапсырма болып табылады. Техникалық тапсырмада ҚА саясаты:

– сыни ақпараттық ресурстарды таңдау;

– сыни ақпараттық ресурстар үшін қауіп-қатерлерді талдау;

– қорғау құралдарына қойылатын талаптарды анықтау;

– ҚА режимін қамтамасыз ету жөніндегі негізгі шешімдерді таңдау;

– қалдық қауіп-қатерді бағалау;

– ұйымның үздіксіз жұмысын қамтамасыз ету бөлімдерімен бірге құжат түрінде ресімделуге тиіс.

Қауіп-қатерлерді талдау жөніндегі, АҚ құралдарына қойылатын талаптарды анықтау жөніндегі және қалдық қауіп-қатерді бағалау жөніндегі ұсынымдар – [2,3,4] бойынша.

ҚР СТ 1201 бойынша ТТ құруға, мазмұнына және баяндалуына қойылатын талаптар.

6.3.4 «Эскиз жоба» сатысын орындау нәтижесі эскиз жоба болып табылады. Құжаттарды орындауға қойылатын талаптар ГОСТ 2.119 бойынша.

6.3.5 «Техникалық жоба» сатысында жұмыстар орындау нәтижесі техникалық жоба болып табылады. Құжаттарды орындауға қойылатын талаптар ГОСТ 2.120 бойынша.

АЖ эскиздік және техникалық жобалау нәтижелері бойынша, қажетіне қарай, ҚР СТ 1201 бойынша бекітілген ТТ-ға өзгерістер енгізу үшін белгіленген тәртіппен ТТ талаптарын түзетуге рұқсат етіледі.

6.3.6 «Жұмыс құжаттамасы» сатысында жұмыстар орындау нәтижесі АЖ жасауға және құрастыруға арналған конструкторлық құжаттама жиынтығы, тапсырыс берушімен келісілген бағдарламалар мен әдістемелер бойынша белгіленген тәртіппен сынақтардан өткен АЖ құрамбөліктері құралдарының тәжірибелік үлгілері, қызметкерлер құрамының және АЖ пайдаланушылардың лауазымдық нұсқаулықтары болып табылады.

6.3.7 «Қолданысқа енгізу» сатысында жұмыстар орындау нәтижесі өнеркәсіптік пайдалануға АЖ қабылдау актісі және АЖ аппараттық және бағдарламалық қамтамасыз етуге сәйкестік сертификаттары, ақпаратты қорғау жөніндегі қолданыстағы нормативтік құжаттардың талаптарына сәйкестігін растау жөніндегі тиісті аккредиттелген органдар берген

ақпаратты криптографикалық қорғайтын және тұтасымен ақпарат жүйесіне арналған құралдар болып табылады.

7 ҚА режимін қамтамасыз етуге арналған АҚ құралдарына қойылатын жалпы талаптар

ҚА режимін қамтамасыз етуге арналған АҚ құралдарына қойылатын жалпы талаптарға:

- атқарымдық талаптар;
- тиімділігіне қойылатын талаптар;
- техникалық талаптар;
- экономикалық талаптар (экономикалық негіздеме);
- пайдалану құжаттамасына қойылатын талаптар кіреді.

7.1 Атқарымдық талаптар

Атқарымдық талаптарға мынадай талаптар тобы:

– өңделетін ақпараттың құпиялық белгісі және АЖ санаты (қорғалу сыныбы);

– ақпаратты қорғау мақсаттар;

– АЖ-де қорғалатын ақпараттың тізімі және оны қорғау тиімділігінің талап етілетін нормалары (деңгейлері);

– Ақпараттың жылыстауы мүмкін арналары және оған санкцияланбаған қол жеткізу тәсілдері, ақпаратқа санкцияланбаған және абайсызда тиетін әсерлер;

– АЖ-де ақпаратты қорғау міндеттері кіреді.

7.1.1 Ақпараттың құпиялық белгісін, АЖ қорғау санатын (қорғалу сыныбын) қолданыстағы нормативтік құжаттар [1] негізінде тапсырыс беруші анықтайды.

7.1.2 Ақпаратты қорғау мақсаты – ақпараттың қауіпсіздігіне қауіп-қатер іске асыру нәтижесінде иеге және/немесе пайдаланушыға келтірілетін зиянның алдын алу немесе көлемін азайту.

Ақпаратты қорғау мақсаты АЖ өмірлік циклінің әрбір сатысы үшін қалыптастырылуға, онда мақсатқа қол жеткізу тиімділігінің көрсеткіші және оның талап етілетін мәні болуға тиіс.

7.1.3 АЖ-де қорғалатын ақпараттың тізімі және оны қорғау тиімділігінің талап етілген деңгейлері (нормалары)

7.1.3.1 АЖ-де қорғалатын ақпараттың нақты тізімі АЖ тағайындауға, АҚ мақсаттарына, АЖ құрамы мен құрылымына сүйеніп, сондай-ақ АҚ құралдарының құрамы мен құрылымымен анықталуға тиіс.

Қорғалатын ақпараттың тізімі тұтасымен АЖ үшін де, сонымен қатар оның құрамбөліктері үшін де анықталады.

7.1.3.2 АҚ тиімділігі жөніндегі талаптарға:

– ақпаратты қорғайтын іске асырылатын тәсілдердің тізімі;

– АҚ тиімділігі көрсеткіштерінің тізімі;

– АҚ тиімділігінің талап етілетін деңгейлері кіреді.

7.1.4 Ақпараттың жылыстауы мүмкін арналарын, оған санкциясыз қол жеткізу тәсілдерін, ақпаратқа санкцияланбаған және абайсызда тиетін әсерлерді анықтау жұмыс жасау алгоритмдерінің құрамын, құрылымын талдау негізінде және АЖ ақпарат қауіпсіздігінің қауіп-қатерлері үлгілерін пайдалана отырып орналастыру шарттары мен қорғалатын ақпаратқа әсер ететін факторлар негізінде жүзеге асырылуға тиіс. Ақпаратқа әсер ететін факторларды жіктеу және олардың атаутізімі – ҚР СТ 1202 бойынша.

7.1.5 Ақпаратты қорғау міндетінің әрқайсысын қалыптастыруға:

– АЖ және оның құрамбөліктері үшін міндеттерді шешу кезінде алды алынуы (жойылуы) қажет қауіпсіздіктің нақты қауіп-қатерінің атауы;

– міндетті шешу тәсілін қалыптастыру;

– нақты міндетті шешу кезінде іске асырылуға тиіс функциялар тізімі;

– міндеті шешу тиімділігіне немесе кепілдіктеріне қойылатын талаптар;

– нақты міндетті шешуге бөлінетін АЖ ресурстарына қойылатын шектеулер кіруге тиіс.

7.1.5.1 АЖ –де АҚ міндеттеріне кіреді:

– техникалық құралдар көмегімен байланыс арналары бойынша берілетін ақпаратты жолдан ұстаудың алдын алу;

– жанама электромагнитті сәулелену және көздеулер есебінен өңделетін ақпараттың жылыстауының алдын алу;

– өңделетін немесе АЖ-де сақталатын қорғалатын ақпаратқа санкциясыз қол жеткізуді болғызбау;

– қорғалатын ақпаратты бұзатын, жоятын, бұрмалайтын немесе АЖ құралдарының жұмыста жаңылысуына әкелетін санкцияланбаған немесе абайсызда болатын әсерлердің алдын алу;

– АЖ техникалық құралдарына енгізілетін ақпаратты жолдан ұстайтын құрылғыларды табу;

– пайдаланушылардың қорғалатын ақпараты және оны тасымалдаушылар бар АЖ жұмысына қол жеткізудің рұқсат етілетін жүйесін ұйымдастыру;

– ақпаратты тасымалдаушыларды жою;

– АЖ-дегі жүйелердің және ақпаратты қорғау құралдарының жұмыс жасауын бақылауды қамтамасыз ету кіреді.

7.2 АҚ тиімділігінің көрсеткіштеріне қойылатын талаптар

АҚ тиімділігінің көрсеткіштерінің тізімі және АҚ тиімділігінің талап етілетін деңгейлері (нормалары) қолданыстағы нормативтік құжаттарда белгіленеді.

7.3 АҚ құралдарына қойылатын техникалық талаптар

АҚ құралдарына қойылатын техникалық талаптарда АЖ қамтамасыз етудің негізгі түрлеріне (техникалық, бағдарламалық), АЖ орнатылатын ғимараттарға (құрылыстарға, үй-жайларға) немесе объектілерге, АЖ аппаратурасы мен жабдығын орналастыруға және құрастыруға, сондай-ақ АҚ құралдарына және АҚ тиімділігін бақылау құралдарына қойылатын талаптар жазылған.

7.3.1 АҚ құралдарына қойылатын талаптарында АЖ атқарымдық тағайындалуы бойынша қолданылатын негізгі техникалық құралдарға сияқты, негізгі техникалық құралдардың жұмыс жасауын қамтамасыз ететін көмекші техникалық құралдарға да қойылатын талаптар бар.

7.3.1.1 Негізгі техникалық құралдарға қойылатын техникалық талаптарда ЖЭМСШК бойынша жылыстаудан, салу құрылғыларынан, ақпаратқа әсер ететін сыртқы және ішкі факторлардан, ақпаратқа санкцияланбаған қол жеткізуден және оған тиетін санкцияланбаған әсерлерден АҚ жөнінде талаптар жазылған.

ҚР СТ 34.013 бойынша ЖЭМСШК бойынша жылыстаудан АҚ жөніндегі талаптар.

7.3.1.2 АЖ техникалық құралдары электрмен қоректендіру ажыратылған жағдайда, апаттарда, сондай-ақ қолайсыз табиғат құбылыстары мен стихиялық апаттар жағдайында ақпараттың сақталуын қамтамасыз етуге тиіс.

7.3.1.3 АЖ техникалық құралдарына қойылатын құрастырылымдық талаптар АҚ жөніндегі талаптарды есепке алып қалыптастырылуға және нақты техникалық құралды әзірлеуге арналған ТТ «Құрастырылымдық талаптар» бөліміне кіргізілуге тиіс.

7.3.1.4 Жерге қосу жүйесіне және электрмен қоректендіру желісіне қойылатын талаптар ҚР СТ 1200 ұсыныстары мен қолданыстағы нормативтік құжаттарға сәйкес белгіленеді.

7.3.1.5 Телекоммуникациялар желісін (деректер беру желісін) құрастыруға қойылатын талаптар қолданыстағы нормативтік құжаттармен регламенттеледі. Жалпы талаптар ҚР СТ 1200 бойынша белгіленеді.

7.3.1.6 ҚА қамтамасыз ететін бағдарламалық-техникалық құралдарға қойылатын АҚ жөніндегі талаптарға мынадай талаптар топтары:

– Қол жеткізуді шектеу бойынша талаптар, міндеттер мен ресурстарды бөлуге қойылатын талаптарды қоса, ақпаратқа және сервистерге қол жеткізуді басқару;

– есепке алуға, күнделікті бақылау мақсаттары үшін елеулі оқиғаларды және зерттеп тексерулерді тіркеуге қойылатын талаптар;

– оларды өңдеудің барлық сатыларындағы сыни маңызды деректердің бүтіндігін тексеру және қамтамасыз ету;

– құпия СҚж-ден қорғау, соның ішінде криптографиялық қорғау құралдарын пайдалану;

– сыни маңызды деректерді резервтік көшіру;

– қол жетімділікке қойылатын жоғарылатын талаптары бар жүйелер үшін істен шығудан кейін АЖ жұмысын қалпына келтіру;

– санкцияланбаған толықтырулардан және өзгертулерден қорғау;

– АЖ құрамында қол жеткізуді шектеуге және есепке алуға қойылатын талаптарды орындауға кепілдік беруге мүмкіндік беретін техникалық және бағдарламалық тетіктердің болу қажеттігін қарастыратын кепілдіктерге қойылатын талаптар кіреді.

7.3.1.7 Ақпаратты өңдеу құралдарына қойылатын талаптар ақпаратқа әсер ететін ішкі факторларға (істен шығу, жаңылысу, қателер) төзімділік бөлігінде ГОСТ 21552 бойынша нақты АЖ және оның құрамбөліктерінің жұмыс істеу сенімділігі мен тұрақтылығы жөніндегі талаптармен бірге белгіленеді.

Ақпаратты өңдеу құралдарын бақылау, сынау және қабылдау әдістері ГОСТ 23773 бойынша белгіленеді.

7.3.2 АЖ орнатылатын ғимараттарға (құрылыстарға, үй-жайларға) немесе объектілерге қойылатын талаптарға бақыланатын аймаққа қойылатын талаптар, ғимараттың (құрылыстың, үй-жайдың) немесе объектінің қоршау құрылымдарына қойылатын, құрылыс технологиясына қойылатын талаптар, коммуникация құралдарына қойылатын талаптар, үй-жайларды экрандауға, дыбыстан оқшаулауға және жабдықты орналастыруға қойылатын талаптар кіреді.

Қорғау ойының мәнін ашатын жобалық құрастырылымдық-технологиялық құжаттама, АҚ техникалық іс-шаралардың негіздемесі аз көлемдегі данамен шығарылады және құрылысқа берілмейді. Бөлімнің ашық атауы – «Қосымша талаптар».

АЖ жабдығын орналастыру техникалық жобада мынадай құжаттамада көрсетіледі:

– бақылау жасалатын аймақтың шекарасы, ақпараттандыру объектісінің орналасқан жері, трансформаторлық қосалқы станциясы, жерге қосатын құрылғысы көрсетілген объектінің инженерлік коммуникацияларының жинақ жоспары(масштабта), бөлгіш құрылғылар мен басқа қорғау элементтерін орнату орындары көрсетілген кабель желілерін төсеу трассасы;

– ақпаратты өңдейтін техникалық құралдарды және режимдік үй-жайларды орналастыру орындары көрсетілген құрылыстардың (объектінің) технологиялық этаж-этаж сызба-жоспары;

– сертификатының бары және орналастырылған орындары көрсетілген ақпаратты өңдейтін орнатылатын құралдардың, АҚ құралдарының және бақылау құралдарының тізімі;

– бөлінген үй-жайлардың тізімі;

– ақпаратты белсенді қорғау жүйелерінің және акустикалық бүркеу құралдарын орналастыру сұлбалары.

7.3.2.1 АЖ орналасатын үй-жайларды (құрылыстарды) объектіні қайта құру және кеңейту қажет кезде АҚ жөніндегі талаптар СНмЕ-ге және қолданыстағы нормативтік құжаттарға сәйкес қойылады.

7.3.2.2 Ақпаратты өңдеу құралдарының жабдықтарын орналастыру бойынша жалпы ұсыныстар - ҚР СТ 1200 бойынша. Ақпаратты өңдейтін негізгі құралдарды орналастыру ғимараттың (объектінің) экрандау қасиеттерін аса көп қолдану арқылы, бақылау жасалатын аймақтың шекарасынан аса алыс қашықтағы төменгі қабаттарда, ішкі үй-жайларда жүргізілуге тиіс.

АЖ құрамбөліктері мен жабдықтарын олар үшін ЭҚ-да орнатылған бақыланатын аймақ шегінде ғана (сертификатталған құралдар үшін), пайдалануға жасалған жазбаша өкімдермен немесе арнайы зерттеулер нәтижелерімен орналастыру керек.

Негізгі жабдық орналастырылған үй-жайларда бақылау жасалатын аймақ шегінен тыс жердегі және қорғау құралдарымен жабдықталмаған, оған қатысы жоқ кабельдер мен сымдарды төсеуге тиым салынады.

Кабельдерді шеткі құрылғыларға қосу кабель экрандары мен шеткі құрылғылардың корпустары арасында сенімді электр түйіспесін қамтамасыз ететін ажыратпалар арқылы жүзеге асырылуға тиіс.

Негізгі құралдардың тізбектері шығарылатын бос қалған ажыратпалар экрандалған қақпақшалармен жабылуға және мөр басылуға, ал ажыратпаларда бос қалған жеке түйіспелер жерге қосылуға тиіс.

Ақпаратты өңдейтін негізгі құралдардың коммутациялық, тарату және келістіруші құрылғылары металл қораптарға немесе шкафтарға салынуға тиіс, қораптар мен шкафтардың қақпақтары сүргі салуға арналған құралдармен және оларды ашуға сигналдаумен жабдықтануға тиіс.

Кабельдердің барлық бос қалған тізбектері қысқаша тұйықталып, бақылау жасалатын аймақ шегінде жерге қосылуға тиіс.

Қорғалатын ақпаратты беру желісі ерекше болуға тиіс, яғни ашық ақпаратты өңдейтін басқа желілерге қосылатын қосылыстары болмауға тиіс.

Пайдалану процесінде қызмет ететін қызметкерлердің қол жеткізуі талап етілмейтін АЖ жабдығы іске қосу-баптау жұмыстарынан кейін жабылып, мөр басылады.

АЖ негізгі техникалық құралдарын құпия келіссөз өткізуге арналған үй-жайларға орналастыру кезінде, діріл және акустикалық арналарымен сөйлеу ақпаратының жылыстауынан қорғау жөнінде шаралар қолданылуға тиіс.

Діріл және акустикалық арналарымен сөйлеу ақпаратының жылыстауынан үй-жайларды қорғау тиімділігін бақылау талаптары мен әдістемесі - ҚР СТ 1171 бойынша.

7.3.2.3 АҚ міндеттерін шешуге бөлінетін АЖ аппараттық, бағдарламалық, ақпараттық, уақытша және басқа ресурстарына шектеулер негізгі бағытталу бойынша АЖ жұмыс жасау тиімділігін рұқсат етілетін деңгейде төмендетуге сүйене отырып, АЖ бар ресурстарын есептеумен анықталады.

7.4 АҚ жөніндегі экономикалық талаптар

АҚ жөніндегі экономикалық талаптарға:

– АЖ және АЖ ҚА жүйелерін құруға жіберілетін рұқсат етілетін шығындар;

– АЖ және АЖ ҚА жүйелерді пайдалануға жіберілетін рұқсат етілетін шығындар кіреді.

7.4.1 ҚА жүйесіне арналған рұқсат етілетін шығындар қорғалатын ақпараттың және қауіпке ұшыратылатын басқа ақпараттық ресурстардың құндылығымен, сондай-ақ ұйымға қауіп-қатерлердің іске асырылуы себебінен болуы мүмкін шығынмен ара қатынаста болуға тиіс.

Тиімділік/құны критерийі бойынша экономикалық көрсеткіштерді талдау нәтижесінде бойынша анализі нәтижесінде АҚ нақты нұсқаларын қолданумен байланысты іс-шаралар бойынша рұқсат етілетін қалдық қауіптер мен шығындар анықталады.

7.5 АҚ жөніндегі пайдалану құжаттамасына қойылатын талаптар

ГОСТ 2.601 бойынша пайдалану құжаттамасына қойылатын жалпы талаптар.

Құжаттардың ҚА режимін қамтамасыз етуге қатысты мынадай атаутізім қосымша әзірленуге тиіс.

7.5.1 Пайдаланушылардың ақпараттық ресурстарға қол жеткізуін басқару жөнінде нұсқаулық.

Нұсқаулық ақпараттық ресурстарға қол жеткізу құқығын беру процесін басқаруды ұйымдастыруға арналған және пайдаланушылардың қол жеткізуді басқарудың өмірлік циклінің барлық кезеңдерінде – жаңа пайдаланушыларды бастапқы тіркеуден бастап ақпараттық сервистерге қол жеткізуді бұдан былай керек етпейтін пайдаланушылардың есептік деректерін жоюға дейін әзірленеді. Пайдаланушыларға жүйелік бақылау құралдарын айналып өтуге

мүмкіндік беретін қол жеткізудің айрықша құқықтарын беру процесін басқаруға ерекше назар аударылуға тиіс.

7.5.2 Қызметкерлердің лауазымдық нұсқаулықтары.

Нұсқаулықтар ҚА қабылданған саясатына сәйкес ҚА қамтамасыз етуге қызметкерлердің міндеттері мен жауапкершіліктерін белгілейді. Нұсқаулықтарда ҚА саясатын іске асыруға немесе қолдауға жүктелетін жалпы жауапкершілік те, сондай-ақ белгілі бір ресурстарды қорғау жөніндегі нақты міндеттер де немесе белгілі процедуралардың немесе қорғау жөніндегі әрекеттердің орындалуына жауапкершілік те сипатталады.

Нұсқаулықтарда (пайдаланушылардың санаттарына қатысты бөлігінде):

– ақпарат тасымалдаушылармен жұмыс;
– ақпарат тасымалдаушыларды жою;
– басқа ұйымдардың өкілдерімен жұмыс бөлімдері бар.

7.5.2.1 «Ақпарат тасымалдаушылармен жұмыс» бөлімі құпия деректердің барлық тасымалдаушыларымен: құжаттармен, есептермен, дискеттермен, қатты дисктермен, компакт дисктермен, флэш-жадымен және басқалармен жұмысты ұйымдастырады.

Бөлімде:

– ақпаратты тасымалдаушылармен жұмыс жасау ережелері және оларды таңбалау;
– тиісті өкілеттіктері бар деректерді алушыларды тіркеу;
– кіріс деректердің толықтығын қамтамасыз ету;
– берілген деректердің (қажеттілігіне қарай) қабылданғанын растау;
– деректерге қол жеткізу берілген тұлғалардың санаты және олардың өкілеттігі;
– тиісті өкілеттігі бар алушы үшін деректердің барлық көшірмелерін таңбалау;
– деректерге қол жеткізу құқықтары бар алушылардың тізімдерін жаңарту тәртібі сипатталуға тиіс.

7.5.2.2 «Ақпаратты тасымалдаушыларды жою» бөлімі ақпаратты тасымалдаушыларды жою тәртібін белгілейді және:

– ақпарат тасымалдаушылар тізімін және олардың сәйкестендіруін;
– әрбір типті (магниттік, қағаз) тасымалдаушылардағы ақпаратты жою (құрту) тәсілін, жою (құрту) кепілдігін тексеруді;
– құпия ақпаратты жоюды (құрту) есепке алу журналын жүргізу тәртібін сипаттауға тиіс.

7.5.3 АЖ басқару жөніндегі нұсқаулық АЖ сенімді жұмысы жөнінде және ҚА режимін қамтамасыз ету жөнінде әкімгердің міндетін сипаттайды. Нұсқаулықта әрбір тапсырманы орындау бойынша АЖ әкімгерінің әрекеттері, соның ішінде:

– деректер файлдарға сүйеніп жасалатын рұқсат етілетін процедуралар;

– тапсырмаларды орындауды жоспарлауға қойылатын талаптар;

– тапсырмаларды орындау кезінде пайда болуы мүмкін қателер мен басқа ерекше жағдайларды өңдеу бойынша әрекеттер, соның ішінде жүйелік утилиттерді пайдалануға қойылатын шектеулер;

– АЖ пайдаланумен байланысты техникалық және басқа мәселелер пайда болған жағдайда көмек сұрау;

– шығыс деректерді алу тәртібі және АЖ жұмысында жаңылысу болған жағдайда шығыс ақпаратты кепілді жою процедурасын қоса, олардың құпиялылығын қамтамасыз ету;

– істен шыққаннан кейін АЖ қайта іске қосу және оның жұмысқа қабілеттілігін қалпына келтіру процедуралары сипатталуға тиіс.

Сондай-ақ нұсқаулықта АЖ қайта іске қосу және тоқтату процедурасы бойынша, деректерді резервті көшіру бойынша, АЖ техникалық қызмет көрсетуі бойынша, егер осы мәселелер дербес құжаттарда сипатталмаса, бөлімдер әзірленуге тиіс.

7.5.4 Пайдалану құжаттамасының жинағына:

– АҚ негізгі және қосымша техникалық құралдарының алғашқы электрмен қоректендіру сұлбасы;

– АҚ негізгі және қосымша техникалық құралдарын жерге қосу сұлбасы;

– АҚ негізгі және қосымша техникалық құралдарының спецификациясы;

– АҚ техникалық құралдарына және АҚ тиімділігін бақылау құралдарына орнатылған бағдарламалық құралдардың спецификациясы;

– кезеңдік бақылауға жататын жабдықтың тізімі, бақылаудағы тексерулердің көлемі және кезеңділігі;

– АЖ формуляры;

– ҚА бойынша формуляр кіруге тиіс.

7.6 АЖ пайдалану кезінде ҚА режимін қамтамасыз ету

АЖ пайдалану процесінде ақпаратқа қол жеткізуді шектеу, жылыстаудың физикалық арналарын бұғаттау және негізгі бағыттары:

– пайдаланушылардың жұмысын бақылау;

– деректердің және бағдарламалардың бүтіндігін қорғау;

– қосымшаларға қол жеткізуді басқару;

– өзгерістерді енгізуді бақылау болып табылатын ҚА саясатын іске асыруды үздіксіз бақылау ұйымдастырылуға тиіс.

7.6.1 Пайдаланушылардың жұмысын бақылау

Пайдаланушылардың жұмысын бақылауға:

– құпия немесе өте маңызды қосымшаларға желілік қосылыстарды бақылау және пайдаланушылардың қол жеткізу өкілеттіктерін бақылау;

– пайдаланушыларды сәйкестендіру және аутентификациялау жолымен жұмыс орындарына қол жеткізуді басқару, сондай-ақ, қажетіне қарай, әрбір тіркелген пайдаланушының терминалы мен орналасқан жері;

– АЖ-ге қол жеткізуге (табысты және табысты емес) ұмтылысты есепке алу журналын жүргізу;

– пайдаланушылардың шарттан тыс уақытта қосылуын шектеу;

– құпия сөздерді таңдауда және пайдалануда ҚА режимін қолдау шараларын бақылау;

– қараусыз қалған жабдықты бақылау және оны санкцияланбаған қол жеткізуден қорғау;

– ҚА бұзылу қаупі жоғары аймақтарда терминалдардың жұмыссыз тұру уақытын қадағалау;

– файлдарды дестемен беру үшін ҚА-қа терминалдың қосу кезеңін шектеу;

– шарттан тыс уақытта жұмыс істеу үшін рұқсат беретін жүйені ұйымдастыру;

– АЖ шығыс ақпаратының кезеңдік талдау және, қажетіне қарай, артық ақпаратты жоюды бақылау кіреді.

7.6.2 Деректердің мен бағдарламалардың бүтіндігін зиянды бағдарламалық қамтамасыз етуден қорғау

7.6.2.1 Вирустардан қорғау:

- ұйым тек лицензиясы бар бағдарламалық қамтамасыз етуді ғана орнатуды талап ететін саясат жүргізуге тиіс;

- вирустарға қарсы бағдарламалық құралдар профилактикалық тексерулер (күнде болса дұрыс) үшін жүйелі жаңартылуға және пайдаланылуға тиіс;

- өте маңызды бағдарламалар мен деректердің бүтіндігін тексеру жүйелі жүргізілуі қажет, артық файлдардың және өзгертулердің санкциясыз енгізілген іздерінің бар екендігі журналда тіркелуге және тергелуге тиіс;

- шыққан тегі белгісіз дискеттер мен басқа ақпаратты ауыспалы тасымалдаушылар пайдалануға дейін вирустың бар-жоғына тексерілуге тиіс;

- АЖ компьютерлік вирустермен зақымдалған жағдайлар туралы хабарлау бойынша және олардың кіруінен болатын зардаптарды жою жөнінде шаралар қолдану бойынша белгіленген процедураларды қатал сақтау;

- вируспен зақымдалу жағдайлары үшін ұйымның үздіксіз жұмыс істеуін қамтамасыз етуді жоспарлау, соның ішінде барлық қажетті деректерді және бағдарламаларды резервтік көшіру жоспарлары және оларды, әсіресе, жұмыс

станцияларының көп мөлшеріне қызмет көрсететін желілік файлды серверлер үшін қалпына келтіру.

7.6.3 Сервистерге қол жеткізуді басқару

7.6.3.1 Электронды поштаны пайдалану кезінде:

– ақпаратты санкцияланбаған жолдан ұстауға және түрлендіруге қатысы бойынша электрондық хабарламалардың осалдығын ескеру;

– дұрыс емес адрестеу немесе хабарлардың тағайындалуы бойынша жіберілмеуі мүмкін екенін, сондай-ақ тұтасымен сервистің сенімділігі мен қол жетімділігін ескеру ұсынылады.

7.6.3.2 Қосымшаларға логикалық қол жеткізу тек тіркелген пайдаланушыларға ғана беріледі. Қосымшалар:

– пайдаланушылардың ұйымда қабылданған қол жеткізуді басқару саясатына сәйкес деректерге және қосымшаларға қол жеткізуді бақылауға;

– бақылау құралдарын айналып өтуге қабілетті жүйелік бағдарламаларға санкцияланбаған қол жеткізуден қорғауды қамтамасыз етуге және СҚ мүмкіндігін қамтамасыз етуге;

– өздері ақпараттық ресурстарды бөлісетін басқа жүйелердің қорғауын бұзбауға тиіс.

7.6.3.3 Бағдарламалық қамтамасыз етуді зақымдау тәуекелін төмендету үшін бағдарламалардың бастапқы мәтіндерінің кітапханасына қол жеткізуге қатаң бақылау жасалуы қажет. Мынадай ережелерді:

– АЖ-де бағдарламалардың бастапқы мәтіндерінің кітапханасын сақтамау;

– бағдарламалардың басылмасын бастапқы мәтіндердің кітапханасында сақтау;

– бағдарламалардың бастапқы мәтіндерінің кітапханасына қол жеткізуді шектеу;

– бағдарламалардың бастапқы мәтіндерінің кітапханаларын жаңарту және бағдарлама мәтіндерін программисттерге беру қосымшаға қол жеткізуге белгіленген нысанда рұқсат алғаннан кейін тек белгіленген жауапты қызметкер ғана жүзеге асыруға тиіс;

– бағдарламалардың бастапқы мәтіндерінің кітапханаларына қол жеткізудің барлық жағдайларын бақылау журналына тіркеу қажет;

– бағдарламалардың бастапқы мәтіндерінің ескірген нұсқаларын оларды пайдалануды аяқтаған күнін көрсетіп барлық көмекші бағдарламалық қамтамасыз етумен және бағдарламалық қамтамасыз етудің осы нұсқасы үшін тапсырмаларды орындауды ұйымдастыру туралы ақпаратпен бірге мұрағаттау керек;

– бағдарламалардың бастапқы мәтіндерінің кітапханаларын ілестіруді және көшіруді өзгерістерді енгізу процесін басқару процедураларына сәйкес жүзеге асыру қажет ережелерін сақтау ұсынылады.

ҚА режимін бұзумен байланысты барлық төтенше жағдайлар мен оқиғаларды журналға тіркеу қажет. Журналды белгіленген уақыт аралығында сақтау керек. Жүйеге кіруге табыссыз ұмтылудан басқа, сондай-ақ табысты қол жеткізу жағдайларын тіркеген де орынды. Бақылау журналына мыналар кіруге тиіс:

– пайдаланушылардың жалпылауыштары;

– жүйеге кіру және шығу уақыты мен күні;

– терминалдың (мүмкіндігі бойынша) жалпылауышы немесе орналасқан орны;

– АЖ-ге қол жеткізуге табысты емес ұмтылулар;

– қалпына келтірілген пайдаланушы жалпылауыштарын санкциясыз пайдалануға ұмтылулар;

– айрықша артық қол жеткізуге рұқсаты бар ресурстарды пайдалану;

– ҚА режимін бұзу көзқарасы тұрғысынан әлуетті қауіпті, жеке әрекеттер;

– құпия ресурстарды пайдалану.

7.6.4 Өзгертулерді енгізу

АЖ-ге және олардың құрамбөліктеріне өзгертулер енгізу бекітілген процедураларға сәйкес, енгізілетін өзгертулердің ҚА режиміне әсерін міндетті бағалаудан кейін жүргізілуге тиіс.

Қажет жағдайларда АЖ сипаттамалары мен параметрлерінің өзгертулер енгізілгеннен кейін белгіленген талаптарға сәйкестігін тексеру мақсатында типтік сынақтар жүргізілуге тиіс.

Типтік сынақтар жүргізудің қажеттігін әзірлеуші қадағалау (бақылау) органдарының келісімі бойынша белгілейді.

Енгізілген өзгертулерді өздері қозғаған тұлғаларға жеткізу ережелері қызметкерлердің нұсқаулықтарында тікелей міндеттерге қатысты бөлігінде анықталуға тиіс.

Қосымша
(анықтамалық)

Библиография

[1] Мемлекеттік құпияларды қорғау жөніндегі нормативтік құқықтық актілердің жинағы. – Астана; Мемлекеттік құпияларды сақтау жөніндегі агенттік, 2002.

[2] ИСО/МЭК 15408-1:2005 Ұсыныстар – Ақпараттық технологиялар. Қорғау әдістері. Ақпараттық технологияларды қорғауды бағалау критерийлері. 1-бөлім. Кіріспе және жалпы үлгі.

[3] ИСО/МЭК 15408-2:2005 Ұсыныстар – Ақпараттық технологиялар. Қорғау әдістері. Ақпараттық технологияларды қорғауды бағалау критерийлері. 2-бөлім. Қауіпсіздіктің пайдалану талаптары.

[4] ИСО/МЭК 15408-3:2005 Ұсыныстар – Ақпараттық технологиялар. Қорғау әдістері. Ақпараттық технологияларды қорғауды бағалау критерийлері. 3-бөлім. Қорғауды қамтамасыз етуге қойылатын талаптар.

ӘОЖ **МСЖ 35.240**

Түйінді сөздер: ақпараттық жүйе, ақпараттық қауіпсіздік, ақпаратты қорғау құралдары, ақпараттық қауіпсіздік режимі, әзірлеу сатылары және кезеңдері

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Защита информации

ТРЕБОВАНИЯ К ПРОЕКТИРОВАНИЮ, УСТАНОВКЕ, НАЛАДКЕ, ЭКСПЛУАТАЦИИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

СТ РК 34.022-2006

Издание официальное

Комитет по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан

Астана

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН ТОО «Специальное конструкторско-технологическое бюро «Гранит»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Председателя Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан от 15 декабря 2006 г. № 550

3 В настоящем стандарте учтены основные нормативные положения следующих международных документов: Рекомендации ИСО/МЭК 15408-1:2005 Технологии информационные. Методы защиты. Критерии оценки защиты информационных технологий. Часть 1. Введение и общая модель. Рекомендации ИСО/МЭК 15408-2:2005 Технологии информационные. Методы защиты. Критерии для оценки защиты информационных технологий. Часть 2. Эксплуатационные требования безопасности. Рекомендации ИСО/МЭК 15408-3:2005 Технологии информационные Методы защиты. Критерии для оценки защиты информационных технологий. Часть 3. Требования к обеспечению защиты

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2011 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Защита информации

ТРЕБОВАНИЯ К ПРОЕКТИРОВАНИЮ, УСТАНОВКЕ, НАЛАДКЕ, ЭКСПЛУАТАЦИИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Дата введения 2008.01.01

1 Область применения

Настоящий стандарт распространяется на информационные системы, используемые в различных видах деятельности, в процессе создания и применения которых осуществляется обработка защищаемой информации, содержащей сведения, отнесенные к государственным секретам [1].

Настоящий стандарт устанавливает порядок разработки, внедрения и эксплуатации информационных систем, отвечающих требованиям информационной безопасности.

Настоящий стандарт применяется в средствах криптографической защиты для повышения гарантий качества защиты информации.

Положения настоящего стандарта подлежат применению государственными органами и организациями Республики Казахстан, взявшими на себя обязательства либо обязанными по статусу выполнять требования правовых документов по защите информации.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК 34.005-2002 Информационная технология. Основные термины и определения.

СТ РК 34.013-2002 Информационная технология. Защита информации от утечки по каналу побочных электромагнитных излучений и наводок при ее обработке на средствах вычислительной техники.

СТ РК 1171-2002 Защита информации. Типовая методика контроля эффективности защиты служебных помещений от акустической разведки по акустическому (речевому) и вибрационному каналам.

СТ РК 1200-2002 Государственная система защиты информации. Технические средства защиты информации, используемые в государственных учреждениях. Технические требования.

СТ РК 1201-2002 Государственная система защиты информации. Порядок разработки, согласования, утверждения и государственной регистрации средств защиты информации.

СТ РК 1202-2002 Государственная система защиты информации. Общие требования к техническим средствам защиты информации. Основные положения.

ГОСТ 2.119-73 ЕСКД. Эскизный проект.

ГОСТ 2.120-73 ЕСКД. Технический проект.

ГОСТ 2.601-95 ЕСКД. Эксплуатационные документы.

ГОСТ 21552-84 Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение

Издание официальное

ГОСТ 23773-88 Машины вычислительные электронные цифровые общего назначения. Методы испытаний.

3 Термины и определения

В настоящем стандарте применены термины с соответствующими определениями, установленные в СТ РК 34.005, а также следующие:

3.1 **Заказчик:** Юридическое лицо (государственное орган или организация независимо от формы собственности), формулирующее требования к ИС, финансирующее работы по ее созданию или по заказам которого осуществляется создание (развитие) и обслуживание ИС.

3.2 **Информационная система:** Система обработки информации совместно с соответствующими организационными ресурсами, такими как человеческие, технические и финансовые ресурсы, предоставляющая и распределяющая информацию.

3.3 **Государственные секреты:** Защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права.

3.4 **Государственная тайна:** Сведения военного, экономического, политического и иного характера, разглашение или утрата которых наносит или может нанести ущерб национальной безопасности Республики Казахстан.

3.5 **Служебная тайна:** Сведения, имеющие характер отдельных данных, которые могут входить в состав государственной тайны, разглашение или утрата которых может нанести ущерб национальным интересам государства, интересам государственных органов и организаций Республики Казахстан.

3.6 **Защищаемая информация:** Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

3.7 **Объект информатизации:** Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, в которых они установлены.

3.8 **Информационная безопасность:** Защищенность информации и оборудования ИС от факторов, представляющих угрозу для конфиденциальности (обеспечение санкционированного доступа), целостности и доступности.

3.9 **Анализ рисков:** Процесс определения угроз безопасности ИС и отдельным ее компонентам, определения их характеристик и потенциального ущерба, а также контрмер.

3.10 **Угрозы информационной безопасности:** Совокупность причин, условий и факторов, создающих опасность объектам информационной безопасности, реализация которых может повлечь нарушение прав, свобод и законных интересов юридических и физических лиц в информационных процессах.

3.11 **Фактор, воздействующий на защищаемую информацию:** Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации или блокирование доступа к ней.

3.12 **Несанкционированное воздействие на информацию:** Воздействие на защищаемую информацию с нарушением установленных прав и/или правил доступа,

приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

3.13 **Непреднамеренное воздействие на информацию:** Ошибка пользователя информацией, сбой технических и программных средств, ИС, а также природные явления или иное нецеленаправленное на изменение информации воздействие, связанное с функционированием технических средств, систем или с деятельностью людей, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования ее носителя.

3.14 **Политика информационной безопасности:** Совокупность документов, определяющих управленческие и проектные решения в области информационной безопасности.

3.15 **Профиль защиты:** Документ, описывающий задачи обеспечения ИБ в терминах функциональных требований и требований гарантированности.

3.16 **Гарантированность механизмов обеспечения ИБ:** Оценка адекватности используемых механизмов обеспечения ИБ выбранным функциональным требованиям. Гарантированность определяется эффективностью и корректностью механизмов обеспечения ИБ.

3.17 **Техническое задание:** Документ, используемый заказчиком в качестве средства для описания и определения задач, выполняемых при реализации договора.

3.18 **Пользователь:** Некто или нечто, посылающий команды и сообщения в ИС и получающий информацию от нее. Пользователями могут быть машины или другие системы, а также люди.

3.19 **Методическое обеспечение ИС:** Документы, которые отражают взаимодействие пользователя с комплексом средств информатизации, включая описание системы и подсистем, методику (технологию) выполнения автоматизированной деятельности, инструкций пользователей.

3.20 **Организационное обеспечение ИС:** Документы (положения, должностные инструкции, штатные расписания, квалификационные требования и др.), устанавливающие организационную структуру, функции и порядок взаимодействия между собой подразделений при работе ИС, в том числе инструкции персоналу.

3.21 **Компонент ИС:** Элемент одного из видов обеспечения (технического, программного, информационного и др.), выполняющий определенную функцию в подсистеме ИС и обеспечивающий ее работу.

3.22 **Оборудование информационных технологий:** Любое оборудование, выполняющее функцию, связанную с вводом, хранением, отображением, поиском, передачей, обработкой, управлением или коммутацией данных и сообщений связи.

3.23 **Режимные помещения:** Помещения, в которых проводятся секретные работы, хранятся секретные документы и изделия, циркулирует иная секретная информация, а также установлены технические средства, предназначенные для ее обработки.

3.24 **Основные технические средства:** Средства вычислительной техники, средства связи, звукозаписи, звукоусиления и звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и размножения документов, кинопроекционная аппаратура, системы электрооборудования и другие средства и системы, используемые для обработки секретной информации или не используемые для обработки секретной информации, но находящиеся в режимных помещениях.

3.25 **Вспомогательные технические средства:** Технические средства, непосредственно не участвующие в обработке секретной информации, но используемые совместно с основными техническими средствами и находящиеся в зоне электромагнитного поля основных технических средств.

4 Обозначения и сокращения

В настоящем стандарте применены обозначения и сокращения:
ИБ – информационная безопасность;
ИС – информационная система;
ЗИ – защита информации;
ТЗ – техническое задание;
ТТЗ – тактико-техническое задание;
НИР – научно-исследовательская работа;
ОКР - опытно-конструкторская работа;
ПЭМИН – побочные электромагнитные излучения и наводки;
СНиП - строительные нормы и правила.

5 Общие положения

5.1 Целесообразность создания и внедрения ИС определяется социальными, научно-техническими или другими полезными эффектами, получаемыми в результате ввода в эксплуатацию ИС.

5.2 Проектирование (модернизация) и внедрение ИС проводится, как правило, в рамках ОКР. Функции основных участников ОКР, взаимоотношения между ними, правила выполнения и порядок реализации законченной ОКР определены СТ РК 1201.

5.3 Проектирование и внедрение вновь создаваемой (модернизируемой) ИС производится в соответствии с ТЗ. ТЗ на ИС является основным документом, определяющим требования, предъявляемые к ИС, порядок создания (модернизации) и приемку при вводе в эксплуатацию.

5.4 В процессе проектирования (модернизации), монтажа и эксплуатации ИС должна быть организована разрешительная система доступа разработчиков, специалистов по монтажу и наладке, пользователей, обслуживающего и эксплуатирующего персонала к техническим, программным средствам и информационным ресурсам ИС. Перечисленные группы специалистов должны иметь допуск к государственным секретам по соответствующей форме.

5.5 Полномочия разработчиков, пользователей, обслуживающего и эксплуатирующего персонала по доступу к ресурсам ИС устанавливаются заказчиком.

5.6 Заказчик, собственник (владелец) ИС, а также организации-участники создания ИС несут ответственность за обеспечение защиты обрабатываемой в ИС информации и выполнение работ по ЗИ на всех стадиях создания и эксплуатации ИС.

5.7 Организации – участники работ по созданию ИС должны иметь лицензию на право проведения работ в области защиты информации. Лицензирование организаций осуществляется в установленном порядке [1].

5.8 Для создания ИС могут применяться как серийно выпускаемые, так и вновь разработанные технические и программные средства обработки информации, а также технические, программные, программно-технические, криптографические средства защиты информации и средства для контроля эффективности ЗИ. Применяемые средства должны иметь сертификаты соответствия по требованиям безопасности информации, выдаваемые соответствующими органами по подтверждению соответствия.

Вновь разработанные средства должны быть сертифицированы в установленном порядке до начала опытной эксплуатации ИС.

5.9 Прекращение эксплуатации ИС предусматривается по следующим основаниям:

- по решению собственника (владельца) ИС, оформленному в установленном порядке;

- согласно принятому решению органа надзора (контроля) из-за несоответствия требованиям нормативных документов по защите информации или другим причинам, приводящим к утечке или другим угрозам защищаемой информации;
- по решению суда.

6 Проектирование информационных систем

6.1 Стадии и этапы создания ИС

Процесс создания ИС представляет собой совокупность работ, упорядоченных во времени, взаимно связанных, объединенных в стадии и этапы. Стадии и этапы создания ИС приведены в таблице 1.

Таблица 1 – Стадии и этапы создания ИС

Стадия создания ИС	Этапы работ
1 Формирование требований к ИС	1.1 Обследование объекта и обоснование необходимости создания ИС. 1.2 Формирование исходных требований заказчика к ИС. 1.3 Оформление отчета о выполненной работе и заявки на разработку ИС.
2 Разработка концепции ИС и концепции ИБ	2.1 Изучение объекта информатизации. 2.2 Проведение НИР (при необходимости). 2.3 Разработка вариантов концепции ИС и вариантов концепции ИБ, выбор варианта концепции ИС и варианта концепции ИБ, удовлетворяющих требованиям заказчика. 2.4 Разработка технического (тактико-технического) задания на аванпроект. 2.5 Оформление отчета о выполненной работе. 2.6 Оформление совместного решения заказчика и исполнителя на разработку аванпроекта.
3 Аванпроект	3.1 Разработка ТЗ на ИС в целом. 3.2 Разработка частных ТЗ на подсистемы ИС.
4 Эскизный проект	4.1 Разработка предварительных проектных решений по выбранному варианту ИС, реализующие механизмы функционирования. 4.2 Разработка документации на ИС и ее части.
5 Технический проект	5.1 Разработка проектных решений по системе и ее компонентам. 5.2 Разработка документации на ИС и ее части. 5.3 Разработка и оформление документов на комплектующие изделия и/или технических заданий (технических требований) на их разработку. 5.4 Разработка заданий на проектирование в смежных частях проекта объекта информатизации.
6 Рабочая документация	6.1 Разработка рабочей документации на ИС и ее компоненты. 6.2 Разработка или адаптация программ.

Окончание таблицы 1

Стадия создания ИС	Этапы работ
7 Ввод в действие	7.1 Подготовка объекта информатизации к вводу ИС в действие. 7.2 Подготовка персонала. 7.3 Комплектация ИС поставляемыми изделиями. 7.4 Строительно-монтажные работы. 7.5 Пусконаладочные работы. 7.6 Проведение предварительных испытаний. 7.7 Проведение опытной эксплуатации. 7.8 Проведение приемочных испытаний.
8 Эксплуатация ИС	8.1 Выполнение работ в соответствии с гарантийными обязательствами. 8.2 Эксплуатация ИС.

6.1.1 Состав, последовательность и сроки реализации стадий и этапов работ, выполняемых при создании (развитии) ИС устанавливают в техническом задании (или в ведомости исполнения договора) на создание (развитие) системы из числа стадий и этапов работ, приведенных в настоящем стандарте.

6.1.2 В зависимости от специфики создаваемой ИС и условий ее создания допускается выполнять отдельные этапы работ до завершения предшествующих стадий и параллельное во времени выполнение этапов работ.

6.1.3 Техническое задание и проектно-сметная документация на разработку ИС в обязательном порядке согласовывается с уполномоченным государственным органом по защите государственных секретов и информационной безопасности, уполномоченными органами в сфере информации и связи и обеспечения национальной безопасности.

6.2 Содержание работ по этапам проектирования

6.2.1 На этапе 1.1 «Обследование объекта и обоснование необходимости создания ИС» в общем случае предусматривается выполнение следующих работ:

- обследование (сбор сведений и анализ) объекта информатизации, оценка состояния режима информационной безопасности (ИБ);
- формулировка требований по обеспечению режима ИБ при реализации функций и задач проектируемой ИС;
- сбор сведений о зарубежных и отечественных аналогах;
- оценку технико-экономической, социальной и т. п. целесообразности создания ИС.

6.2.2 На этапе 1.2 «Формирование исходных требований заказчика к ИС» проводят подготовку исходных данных для формирования требований к ИС:

- характеристику объекта информатизации;
- функции и задачи создаваемой ИС;
- условия функционирования ИС (требования к климатическим и механическим воздействиям);
- требования к обеспечению режима ИБ по каждой функции и задаче ИС (период недоступности, время доступа и другие показатели, определяемые предметной областью; показатели надежности, хранения, доставки; градации конфиденциальности информации);
- условия создания и эксплуатации ИС;
- ограничение допустимых затрат на разработку;

- проведение НИР (при необходимости);
- формулировку и оформление требований к ИС.

6.2.3 На этапе 1.3 «Оформление отчета о выполненной работе и заявки на разработку ИС» проводят оформление отчета о выполненных работах на данном этапе и оформляют заявку на разработку ИС или другого заменяющего ее документа.

6.2.4 На этапах 2.1 «Изучение объекта информатизации» и 2.2 «Проведение НИР» организация – исполнитель НИР проводит детальное исследование объекта информатизации и необходимые НИР, связанные с поиском путей и оценкой возможности реализации требований заказчика, оформляют и утверждают отчеты по проведенным НИР.

6.2.5 На этапе 2.3 «Разработка вариантов концепции ИС и концепции ИБ, выбор варианта концепции ИС и варианта концепции ИБ, удовлетворяющих требованиям заказчика» проводят:

- анализ правовых и договорных требований;
- разработку альтернативных вариантов концепции ИС, альтернативных вариантов концепции ИБ и планов их реализации;
- анализ угроз (классы рисков) которым могут подвергаться информационные ресурсы системы;
- оценку необходимых ресурсов на реализацию альтернативных вариантов и обеспечение функционирования;
- оценку преимуществ и недостатков каждого из вариантов;
- сопоставление требований заказчика и характеристик предлагаемого варианта ИС;
- выбор оптимального варианта концепции ИС и выбор оптимального варианта концепции ИБ;
- определение порядка оценки качества и условий приемки ИС;
- оценку эффектов, получаемых от ИС.

6.2.6 На этапе 2.4 «Разработка технического (тактико-технического) задания на аванпроект» проводится разработка, согласование и утверждение ТЗ (ТТЗ) на аванпроект и, при необходимости, технические задания на составные части ИС.

6.2.7 На этапе 2.5 «Оформление отчета о выполненной работе» подготавливается и оформляется отчет, содержащий описание выполненных работ на стадии, описание и обоснование предлагаемого варианта концепции ИС и предлагаемого варианта концепции ИБ.

6.2.8 На этапе 2.6 «Оформление совместного решения заказчика и исполнителя на разработку аванпроекта» заключается договор или оформляется совместное решение заказчика и исполнителя на разработку аванпроекта.

6.2.9 Этап 3.1 «Разработка ТЗ на ИС» и этап 3.2 «Разработка частных ТЗ на подсистемы ИС» предусматривает выполнение работ 6.2.9.1 – 6.2.9.8

6.2.9.1 Техническое обоснование целесообразности создания ИС, проработка вопросов ее применения.

6.2.9.2 Определение технических возможностей, путей создания ИС, рассмотрение возможных вариантов технических решений, обоснование выбора оптимального варианта и состава ИС.

6.2.9.3 Формирование требований к ИС:

- общие технические требования;
- требования к функциям ИС;
- требования к техническому обеспечению;
- требования к программному обеспечению;
- требования к информационному обеспечению;
- требования к лингвистическому обеспечению;

- требования к организационному обеспечению;
- требования к методическому обеспечению;
- описание угроз информации;
- задачи защиты информации в ИС;
- перечень защищаемой информации и требуемые нормы (уровни) эффективности ее защиты;
- выбор элементов системы, для которых будет производиться анализ рисков;
- профиль защиты и требования к средствам ЗИ;
- требования к обеспечению режима ИБ;
- требования по обеспечению бесперебойной работы организации;
- требования к подготовленности персонала;
- требование к правовому обеспечению;
- требования к документации.

6.2.9.4 Сопоставление проектируемой ИС с аналогичными отечественными и зарубежными образцами по показателям, согласованным с заказчиком.

6.2.9.5 Определение образцов компонентов ИС для проведения испытаний.

6.2.9.6 Расчет лимитной стоимости выполнения ОКР и ориентировочных затрат на эксплуатацию ИС.

6.2.9.7 Разработка ТЗ на ОКР по созданию ИС.

6.2.9.8 Составление отчетной документации по результатам выполнения аванпроекта с обоснованием принимаемых по нему решений.

6.2.10 Стадия «Эскизный проект» предусматривает выполнение этапов работ 4.1 и 4.2 на этапе разработки эскизного проекта ОКР.

6.2.10.1 На этапе 4.1 «Разработка предварительных проектных решений по выбранному варианту ИС, реализующие механизмы функционирования» определяются:

- функции ИС;
- функции подсистем, их цели и эффекты;
- состав комплексов задач и отдельных задач;
- концепция информационной базы, ее укрупненная структура;
- функции системы управления базой данных и состав вычислительной системы;
- функции и параметры основных программных средств;
- технические решения по структуре системы и подсистем, обеспечивающих режим ИБ, уровни иерархии и система управления ИБ;
- технические решения по режимам функционирования и диагностике состояний системы, обеспечивающей режим ИБ;
- описание показателей, характеризующих качество системы, обеспечивающих режим ИБ и методы их измерения;
- перечень угроз ИБ, для которых обеспечивается защита в рамках предлагаемого проектного решения.

6.2.10.2 На этапе 4.2 «Разработка документации на ИС и ее части» проводят разработку, оформление, согласование и утверждение документации в объеме, необходимом для описания полной совокупности принятых решений и достаточном для дальнейшего выполнения работ по созданию ИС.

В пояснительной записке приводится обоснование выбора технических средств обеспечивающих в пусковом, нормальном и аварийных режимах функционирование информационной системы и технических средств ЗИ и режим ИБ.

6.2.11 Стадия «Технический проект» реализуется на этапе разработки технического проекта ОКР и включает в себя этапы 5.1 – 5.4.

6.2.11.1 На этапе 5.1 «Разработка проектных решений по системе и ее компонентам» обеспечивают разработку общих решений по ИС и ее частям, функционально –

алгоритмической структуре системы, по функциям персонала и организационной структуре, по структуре технических средств, по алгоритмам решений задач и применяемым языкам, по организации и ведению информационной базы, по программному обеспечению, по организации сбора и передачи данных.

6.2.11.2 На этапе 5.2 «Разработка документации на ИС и ее части» производится разработка окончательных решений по общесистемным вопросам, в том числе по структурам ИС и по видам обеспечения.

В части ИБ на этапе должны быть разработаны:

- должностные инструкции персонала, регламентирующие вопросы доступа в помещения и к оборудованию, работу с носителями информации, доступ к информации;
- правила администрирования в ИС;
- правила работы пользователей в ИС;
- правила работы со сторонними организациями.

Должен быть разработан план мероприятий по обеспечению режима ИБ с рассмотрением основных составляющих комплексной системы защиты:

- организация работы персонала;
- физическая защита и контроль соблюдения режима ИБ;
- организация доступа в многопользовательской системе;
- поддержание работоспособности и обеспечение ИБ в сетях;
- планирование восстановительных работ.

Результаты работы должны быть изложены в техническом проекте «Средства защиты информации и средства контроля эффективности защиты» как разделе технического проекта ИС.

6.2.11.3 На этапе 5.3 «Разработка и оформление документов на комплектующие изделия и/или технических заданий (технических требований) на их разработку» проводят:

- подготовку и оформление документации на поставку изделий для комплектования ИС;
- определение технических требований и составление ТЗ на разработку изделий, не поставляемых серийно;
- разработку технических заданий на средства защиты информации и изготовление опытных образцов;
- разработку технических заданий на средства контроля эффективности защиты информации и изготовление опытных образцов.

6.2.11.4 На этапе 5.4 «Разработка заданий на проектирование в смежных частях проекта объекта информатизации» осуществляют разработку, оформление, согласование и утверждение заданий на проектирование в смежных частях проекта ИС для проведения строительных, электротехнических, коммуникационных, санитарно-технических и других подготовительных работ, связанных с созданием ИС.

6.2.12 На этапе 6.1 «Разработка рабочей документации на ИС и ее компоненты» проводят разработку рабочей документации, содержащей все необходимые и достаточные сведения для обеспечения выполнения работ по вводу ИС в действие и ее эксплуатацию, а также для поддержания уровня эксплуатационных характеристик системы в соответствии с принятыми проектными решениями, ее оформление, согласование и утверждение.

Должен быть разработан план мероприятий по обеспечению режима ИБ, содержащий разделы:

- организация работы персонала;
- физическая защита ИС и контроль соблюдения ИБ;
- организация доступа в многопользовательской системе;

- поддержание работоспособности и обеспечение ИБ в сетях;
- планирование восстановительных работ.

Должны быть разработаны:

- должностные инструкции персонала, регламентирующие вопросы доступа в помещения и к оборудованию, работу с носителями информации, доступ к информации, уничтожение носителей информации;
- правила администрирования в ИС;
- правила работы пользователей в ИС;
- правила работы со сторонними организациями.

Также на этом этапе должны быть изготовлены опытные образцы компонентов, изготовленных по ТЗ в рамках конкретной ОКР на ИС и проведены их испытания.

На этапе 6.2 «Разработка или адаптация программ» проводят разработку программ и программных средств системы, выбор, адаптацию и/или привязку приобретаемых средств, подтверждение соответствия приобретенных программных средств установленным требованиям информационной безопасности, проводимое соответствующими аккредитованными органами по подтверждению соответствия.

Должны быть приведены технические решения по организации сбора и передачи данных, а также технические решения по программному обеспечению, относящиеся к режиму ИБ.

6.2.13 На этапе 7.1 «Подготовка объекта информатизации к вводу ИС в действие» проводят работы по организационной подготовке объекта информатизации к вводу ИС в действие, в том числе:

- реализацию проектных решений по организационной структуре ИС;
- обеспечение подразделений инструктивно-методическими материалами;
- внедрение классификаторов информации;
- выявление критически важных функций и систем, определяющих ИБ в ИС;
- определение перечня возможных аварий и их последствий для ИБ;
- разработка мер ИБ, направленных на ликвидацию последствий нарушений в работе, вызванных стихийными бедствиями, авариями, атаками нарушителей.

В многопользовательской системе также должны быть решены вопросы доступа в ИС:

- регистрация пользователей;
- управление паролями пользователей;
- управление привилегиями;
- пересмотр прав доступа пользователей;
- управление привилегированным доступом для администрирования системы, в том числе системы ИБ.

В процессе подготовки к эксплуатации должна быть организована физическая защита объекта информатизации и организован контроль соблюдения режима ИБ в части вопросов:

- доступ в помещения;
- сохранение конфиденциальности;
- ведение журналов регистрации событий - учет попыток доступа (успешных и неудачных) в ИС;
- организация доступа к носителям информации и их защите (регистрация пользователей, управление привилегиями; управление пользовательскими паролями; пересмотр прав доступа пользователей; отслеживание времени простоя терминалов и защита пользовательского оборудования, оставленного без присмотра; ограничение доступа к сервисам; ограничение допустимого периода подключения);
- доступ к документации по ИС.

На этапе 7.2 «Подготовка персонала» проводят обучение персонала и проверку его подготовленности обеспечить функционирование ИС, а также должны быть решены вопросы доступа пользователей к работе в ИС, организации физической защиты и контроля за соблюдением режима ИБ.

На этапе 7.3 «Комплектация ИС поставляемыми изделиями» обеспечивают получение комплектующих изделий серийного и единичного производства, материалов и монтажных изделий. Проводится входной контроль их качества и подтверждение соответствия установленным требованиям информационной безопасности.

На этапе 7.4 «Строительно-монтажные работы» проводят:

- выполнение работ по строительству специализированных помещений (зданий, сооружений) для размещения технических средств и персонала ИС;
- сооружение кабельных каналов;
- выполнение работ по монтажу технических средств и линий связи;
- испытание смонтированных технических средств;
- сдачу смонтированных технических средств для проведения пусконаладочных работ.

На этапе 7.5 «Пусконаладочные работы» проводят автономную отладку технических и программных средств, загрузку информации в базу данных и проверку системы ее ведения, комплексную наладку всех средств системы. В процессе проведения работ должен быть организован контроль:

- доступа в помещения;
- сохранения конфиденциальности;
- ведения журналов регистрации событий;
- организации доступа к носителям информации;
- доступа к документации по ИС.

Пусконаладочные работы должны проводиться с применением несекретной (условной) информации.

На этапе 7.6 «Проведение предварительных испытаний» осуществляют:

- испытания ИС на работоспособность и соответствие техническому заданию в соответствии с программой и методикой предварительных испытаний;
- проверку реагирования ИС на чрезвычайные ситуации и переход на аварийный режим работы;
- проверку программно-технических механизмов ИБ во всех режимах работы ИС при выполнении функций и решении контрольных задач;
- устранение неисправностей и внесение изменений в конструкторскую документацию на ИС;
- оформление протоколов испытаний и акта о приемке ИС в опытную эксплуатацию.

На этапе 7.7 «Проведение опытной эксплуатации» проводят:

- опытную эксплуатацию ИС;
- анализ результатов опытной эксплуатации;
- доработку (при необходимости) программного обеспечения ИС, средств защиты информации и средств контроля эффективности защиты информации;
- комплексную отладку технических средств ЗИ во всех режимах работы, включая аварийные режимы ИС;
- оформление акта о завершении опытной эксплуатации ИС.

На этапе 7.8 «Проведение приемочных испытаний» проводят:

- проведение испытаний на соответствие ТЗ в соответствии с утвержденной в установленном порядке программой и методикой приемочных испытаний;
- анализ результатов испытаний и устранение недостатков, выявленных в процессе испытаний;

- оформление протоколов испытаний и акта о приемке ИС в эксплуатацию;
- приемку разработанной ИС администратором бюджетной программы в установленном законодательством порядке;
- проведение отраслевой оценки ИС уполномоченным органом в сфере информатизации и связи в соответствии с нормативными правовыми актами.

Датой ввода ИС в эксплуатацию считают дату подписания акта о вводе ИС в действие приемочной комиссией.

Применение ИС для обработки защищаемой информации разрешается только после подтверждения ее соответствия установленным требованиям безопасности информации, проводимое соответствующими аккредитованными органами по подтверждению соответствия.

Решение о возможности применения ИС принимает заказчик на основании акта комиссии по проведению приемочных испытаний системы.

6.2.14 На этапе 8.1 «Выполнение работ в соответствии с гарантийными обязательствами» осуществляют работы по устранению недостатков, выявленных при эксплуатации ИС в течение установленных гарантийных сроков, внесению необходимых изменений в документацию на ИС.

На этапе 8.2 «Эксплуатация ИС» осуществляют работы по:

- анализу функционирования ИС;
- выявлению отклонений фактических эксплуатационных характеристик от проектных значений и установлению причин этих отклонений;
- устранению выявленных недостатков и обеспечению стабильности эксплуатационных характеристик и ИБ;
- внесению изменений в конструкторскую документацию в соответствии с утвержденными процедурами и правилами доведения внесенных изменений до сведения лиц, которых они затрагивают.

6.3 Результаты выполнения работ по стадиям

6.3.1 Результатом выполнения стадии «Формирование требований к ИС» являются научно-технический отчет, техническое задание на аванпроект, технико-экономическое обоснование и заявка на создание ИС.

6.3.2 Результатом выполнения стадии «Разработка концепции ИС и концепции ИБ» является отчет. В отчете, разрабатываемом на этой стадии, в разделе «Функции и задачи создаваемой ИС» должен присутствовать подраздел «Требования к обеспечению режима ИБ». В нем должны быть описаны требования к обеспечению режима ИБ по каждой функции и задаче ИС.

После выбора варианта концепции создаваемой ИС должна быть разработана концепция ИБ на основе анализа следующих групп факторов:

- правовые и договорные требования;
- требования к обеспечению режима ИБ по функциям и задачам ИС;

По результатам анализа формулируются общие положения ИБ, затрагивающие организацию в целом:

- цели и приоритеты, которые преследует организация в области ИБ;
- общие направления в достижении этих целей;
- аспекты программы ИБ, которые должны решаться на уровне организации в целом;
- должностные лица и их обязанности по реализации программы ИБ.

Концепция политики ИБ должна быть оформлена в виде отчета.

6.3.3 Результатом выполнения стадии «Аванпроект» является техническое задание на создание ИС. В техническом задании должна быть документально оформлена политика ИБ с содержанием разделов:

- выбор критичных информационных ресурсов;
- анализ рисков для критичных информационных ресурсов;
- определение требований к средствам защиты;
- выбор основных решений по обеспечению режима ИБ;
- оценка остаточного риска;
- обеспечение бесперебойной работы организации.

Рекомендации по анализу рисков, определению требований к средствам ЗИ и оценке остаточного риска – по [2,3,4].

Требования к построению, содержанию и изложению ТЗ по СТ РК 1201.

6.3.4 Результатом выполнения стадии «Эскизный проект» является эскизный проект. Требования к выполнению документов по ГОСТ 2.119.

6.3.5 Результатом выполнения работ на стадии «Технический проект» является технический проект. Требования к выполнению документов по ГОСТ 2.120.

По результатам эскизного и технического проектирования ИС допускается, при необходимости, корректировать требования ТЗ в порядке, установленном для внесения изменений в утвержденное ТЗ по СТ РК 1201.

6.3.6 Результатом выполнения работ на стадии «Рабочая документация» является комплект конструкторской документации для изготовления и монтажа ИС, опытные образцы средств компонентов ИС прошедшие испытания в установленном порядке по программам и методикам согласованных с заказчиком, должностные инструкции персонала и пользователей ИС.

6.3.7 Результатом выполнения работ на стадии «Ввод в действие» является акт приемки ИС в промышленную эксплуатацию и сертификаты соответствия на аппаратное и программное обеспечение ИС, средства криптографической защиты информации и на информационную систему в целом, выданные соответствующими аккредитованными органами по подтверждению соответствия требованиям действующих нормативных документов по защите информации.

7 Общие требования к средствам ЗИ для обеспечения режима ИБ

Общие требования к средствам ЗИ для обеспечения режима ИБ включают:

- функциональные требования;
- требования к эффективности;
- технические требования;
- экономические требования (экономическое обоснование);
- требования к эксплуатационной документации.

7.1 Функциональные требования

Функциональные требования включают в себя следующие группы требований:

- грифы секретности обрабатываемой информации и категорию (класс защищенности) ИС;
- цели защиты информации;
- перечень защищаемой в ИС информации и требуемые нормы (уровни) эффективности ее защиты;
- возможные каналы утечки информации и способы несанкционированного доступа к ней, несанкционированные и непреднамеренные воздействия на информацию;

- задачи защиты информации в ИС.

7.1.1 Гриф секретности информации, категорию защиты (класс защищенности) ИС определяет заказчик на основании действующих нормативных документов [1].

7.1.2 Цель защиты информации – предотвращение или снижение величины ущерба, наносимого владельцу и/или пользователю, вследствие реализации угроз безопасности информации.

Цель защиты информации должна формулироваться для каждой стадии жизненного цикла ИС, иметь показатель эффективности достижения цели и требуемое его значение.

7.1.3 Перечень защищаемой в ИС информации и требуемые (нормы) уровни эффективности ее защиты

7.1.3.1 Конкретный перечень защищаемой информации в ИС должен определяться исходя из назначения ИС, целей ЗИ, состава и структуры ИС, а также составом и структурой средств ЗИ.

Перечень защищаемой информации определяется как для ИС в целом, так и для ее компонентов.

7.1.3.2 Требования по эффективности ЗИ должны включать:

- перечень реализуемых способов защиты информации;
- перечень показателей эффективности ЗИ;
- требуемые уровни эффективности ЗИ.

7.1.4 Выявление возможных каналов утечки информации, способов несанкционированного доступа к ней, несанкционированных и непреднамеренных воздействий на информацию должно осуществляться на основе анализа состава, структуры, алгоритмов функционирования и условий размещения ИС с использованием моделей угроз безопасности информации и факторов, воздействующих на защищаемую информацию. Классификация и номенклатура факторов, воздействующих на информацию - по СТ РК 1202.

7.1.5 Формулировка каждой задачи защиты информации должна включать:

- наименование конкретной угрозы безопасности для ИС и ее компонентов, которую необходимо предотвратить (устранить) при решении задачи;
- формулировку способа решения задачи;
- перечень функций, которые должны быть реализованы при решении конкретной задачи;
- требования к эффективности или гарантиям решения задачи;
- ограничения на ресурсы ИС, выделяемые на решение конкретной задачи.

7.1.5.1 Задачи ЗИ в ИС включают:

- предотвращение перехвата информации, передаваемой по каналам связи с помощью технических средств;
- предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок;
- исключение несанкционированного доступа к обрабатываемой или хранящейся в ИС защищаемой информации;
- предотвращение несанкционированных или непреднамеренных воздействий, вызывающих разрушение, уничтожение, искажение защищаемой информации или сбои в работе средств ИС;
- выявление устройств перехвата информации, внедряемых в технические средства ИС;
- организацию разрешительной системы допуска пользователей ИС к работе с защищаемой информацией и ее носителями;
- уничтожение носителей информации;

- осуществление контроля функционирования систем и средств защиты информации в ИС.

7.2 Требования к показателям эффективности ЗИ

Перечень показателей эффективности ЗИ и требуемые уровни (нормы) эффективности ЗИ устанавливаются действующими нормативными документами.

7.3 Технические требования к средствам ЗИ

Технические требования к средствам ЗИ содержат требования к основным видам обеспечения ИС (техническому, программному), к зданиям (сооружениям, помещениям) или объектам, в которых ИС устанавливается, к размещению и монтажу аппаратуры и оборудования ИС, а также к средствам ЗИ и средствам контроля эффективности ЗИ.

7.3.1 Требования к средствам ЗИ содержат требования как к основным техническим средствам, применяемым по функциональному предназначению ИС, так и к вспомогательным техническим средствам, обеспечивающим функционирование основных технических средств.

7.3.1.1 Технические требования, предъявляемые к основным техническим средствам, содержат требования по ЗИ от утечки по ПЭМИН, от закладочных устройств, от внешних и внутренних факторов воздействующих на информацию, от несанкционированного доступа к информации и несанкционированных воздействий на нее.

Требования по ЗИ от утечки по ПЭМИН по СТ РК 34.013.

7.3.1.2 Технические средства ИС должны обеспечивать сохранность информации при отключении электропитания, при авариях, а также в условиях неблагоприятных природных явлений и стихийных бедствий.

7.3.1.3 Конструктивные требования, предъявляемые к техническим средствам ИС, должны формироваться с учетом требований по ЗИ и включаться в раздел «Конструктивные требования» ТЗ на разработку конкретного технического средства.

7.3.1.4 Требования к системе заземления и сети электропитания должны устанавливаться в соответствии с рекомендациями СТ РК 1200 и требованиями действующих нормативных документов.

7.3.1.5 Требования к монтажу сети телекоммуникаций (сети передачи данных) регламентируются действующими нормативными документами. Общие требования устанавливаются по СТ РК 1200.

7.3.1.6 Требования по ЗИ к программно-техническим средствам обеспечения ИБ включают группы требований:

- требования по разграничению доступа, управление доступом к информации и сервисам, включая требования к разделению обязанностей и ресурсов;
- требования к учету, регистрации значительных событий для целей повседневного контроля и расследований;
- проверка и обеспечение целостности критически важных данных на всех стадиях их обработки;
- защита конфиденциальных данных от НСД, в том числе использование средств криптографической защиты;
- резервное копирование критически важных данных;
- восстановление работы ИС после отказов для систем с повышенными требованиями к доступности;
- защита от несанкционированных дополнений и изменений;

- требования к гарантиям, предусматривающие необходимость наличия в составе ИС технических и программных механизмов, позволяющих гарантировать выполнение требований к разграничению доступа и к учету.

7.3.1.7 Требования к средствам обработки информации в части устойчивости к внутренним факторам, воздействующим на информацию (отказы, сбои, ошибки) устанавливают совместно с требованиями по надежности и устойчивости функционирования конкретной ИС и ее компонентов по ГОСТ 21552.

Методы контроля, испытаний и приемки средств обработки информации устанавливают по ГОСТ 23773.

7.3.2 Требования к зданиям (сооружениям, помещениям) или объектам, в которых устанавливаются ИС, включают требования к контролируемой зоне, требования к ограждающим конструкциям здания (сооружения, помещения) или объекта, к технологии строительства, требования к средствам коммуникаций, требования к экранированию, звукоизоляции помещений и размещению оборудования.

Проектная конструкторско-технологическая документация, раскрывающая сущность замысла защиты, обоснование технических мероприятий ЗИ выпускается в ограниченном количестве экземпляров и на строительство не выдается. Открытое наименование раздела - «Дополнительные требования».

Размещение оборудования ИС отражается в техническом проекте в следующей документации:

- сводный план инженерных коммуникаций объекта (в масштабе) с указанием границы контролируемой зоны, местоположение объекта информатизации, трансформаторной подстанции, заземляющего устройства, трасс прокладки кабельных линий с указанием мест установки разделительных устройств и других элементов защиты;
- технологические поэтажные планировки сооружений (объекта) с указанием мест размещения технических средств обработки информации и режимных помещений;
- перечень устанавливаемых средств обработки информации, средств ЗИ и средств контроля с указанием наличия сертификата и мест их установки;
- перечень выделенных помещений;
- схемы систем активной защиты информации и размещения устройств акустической маскировки.

7.3.2.1 При необходимости реконструкции и расширения помещений (сооружений) объекта, в котором размещается ИС, требования по ЗИ предъявляются в соответствии со СНиП и другими действующими нормативными документами.

7.3.2.2 Общие рекомендации по размещению оборудования средств обработки информации - по СТ РК 1200. Размещение основных средств обработки информации должно производится с максимальным использованием экранирующих свойств здания (объекта), на нижних этажах, во внутренних помещениях на максимальном удалении от границ контролируемой зоны.

Компоненты и оборудование ИС следует размещать только в пределах контролируемой зоны, установленной для них в ЭД (для сертифицированных средств), предписаниями на эксплуатацию или результатами специсследований. Режимные помещения необходимо размещать на максимальных расстояниях от границ контролируемой зоны.

В помещениях, где установлено основное оборудование, запрещается прокладывать не относящиеся к нему кабели и провода, выходящие за пределы контролируемой зоны и не оборудованные средствами защиты.

Подключение кабелей к оконечным устройствам должно осуществляться через разъемы, обеспечивающие надежный электрический контакт между экранами кабелей и корпусами оконечных устройств.

Незадействованные разъемы, на которые выводятся цепи основных средств, должны закрываться экранирующими заглушками и опечатываться, а незадействованные отдельные контакты в разъемах – заземляться.

Коммутационные, распределительные и согласующие устройства основных средств обработки информации должны размещаться в металлических коробках или шкафах, крышки коробок и шкафов должны оборудоваться приспособлениями для опечатывания и сигнализацией на вскрытие.

Все свободные цепи кабелей должны быть замкнуты накоротко и заземлены в пределах контролируемой зоны.

Сеть передачи защищаемой информации должна быть выделенной, то есть не иметь подключений к другим сетям, в которых производится обработка открытой информации.

Оборудование ИС, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после пусконаладочных работ закрывается и опечатывается.

При размещении основных технических средств ИС в помещениях, предназначенных для ведения конфиденциальных переговоров, должны быть приняты меры по защите от утечки речевой информации по вибрационным и акустическим каналам.

Требования и методика контроля эффективности защиты помещений от утечки речевой информации по вибрационным и акустическим каналам – по СТ РК 1171.

7.3.2.3 Ограничения на аппаратные, программные, информационные, временные и другие ресурсы ИС, выделяемые на решение задач ЗИ, определяются с учетом имеющихся ресурсов ИС исходя из допустимого снижения эффективности функционирования ИС по основному предназначению.

7.4 Экономические требования по ЗИ

Экономические требования по ЗИ включают:

- допустимые затраты на создание ИС и системы ИБ ИС;
- допустимые затраты на эксплуатацию ИС и системы ИБ ИС.

7.4.1 Допустимые затраты на систему ИБ должны соотноситься с ценностью защищаемой информации и других информационных ресурсов, подвергающихся риску, а также с ущербом, который может быть нанесен организации из-за реализации угроз.

В результате анализа экономических показателей по критерию эффективность/стоимость уточняются допустимые остаточные риски и расходы по мероприятиям, связанным с применением конкретных вариантов ЗИ.

7.5 Требования к эксплуатационной документации по ЗИ

Общие требования к эксплуатационной документации по ГОСТ 2.601.

Дополнительно должна быть разработана следующая номенклатура документов, относящаяся к обеспечению режима ИБ.

7.5.1 Инструкция по управлению доступом пользователей к информационным ресурсам.

Инструкция предназначена для организации управления процессом предоставления прав доступа к информационным ресурсам и разрабатывается на все стадии жизненного цикла управления доступом пользователей - от начальной регистрации новых пользователей до удаления учетных данных пользователей, которые не нуждаются больше в доступе к информационным сервисам. Особое внимание должно быть уделено управлению процессом предоставления привилегированных прав доступа, которые позволяют пользователям обойти средства системного контроля.

7.5.2 Должностные инструкции персонала.

Инструкции устанавливают обязанности и ответственность персонала за обеспечение ИБ в соответствии с принятой политикой ИБ. В инструкциях отражается как общая ответственность за реализацию или поддержку политики ИБ, так и конкретные обязанности по защите определенных ресурсов или ответственность за выполнение определенных процедур или действий по защите.

Инструкции содержат разделы (в части касающейся категорий пользователей):

- работа с носителями информации;
- уничтожение носителей информации;
- работа с представителями сторонних организаций.

7.5.2.1 Раздел «Работа с носителями информации» организует работу со всеми носителями конфиденциальных данных: документами, отчетами, дискетами, жесткими дисками, компакт дисками, флэш-памятью и проч.

В разделе должно быть отражено:

- правила работы с носителями информации и их маркировка;
- регистрация получателей данных, имеющих соответствующие полномочия;
- обеспечение полноты входных данных;
- подтверждение получения переданных данных (по необходимости);
- категория лиц, которым предоставлен доступ к данным и их полномочия;
- маркировка всех копий данных для получателя, имеющего соответствующие полномочия;
- порядок обновления списков получателей с правом доступа к данным.

7.5.2.2 Раздел «Уничтожение носителей информации» определяет порядок уничтожения носителей информации и должен отражать:

- перечень носителей информации и их идентификацию;
- способ удаления (уничтожения) информации на носителях каждого типа (магнитные, бумажные), проверка гарантий удаления (уничтожения);
- порядок ведения журнала учета уничтожения (удаления) конфиденциальной информации.

7.5.3 Инструкция по администрированию ИС отражает обязанности администратора по надежной работе ИС и обеспечению режима ИБ. В инструкции должны быть описаны действия администратора ИС по выполнению каждого задания, в том числе:

- допустимые процедуры оперирования с файлами данных;
- требования к планированию выполнения заданий;
- действия по обработке ошибок и других исключительных ситуаций, которые могут возникать при выполнении зданий, в том числе ограничения на использование системных утилит;
- обращения за помощью в случае возникновения технических и других проблем, связанных с эксплуатацией ИС;
- порядок получения выходных данных и обеспечение их конфиденциальности, включая процедуры гарантированного удаления выходной информации в случае сбоя в работе ИС;
- процедуры перезапуска и восстановления работоспособности ИС после отказа.

В инструкции также должны быть разработаны разделы по процедуре перезапуска и остановки ИС, резервному копированию данных, техническому обслуживанию ИС, если эти вопросы не отражены в самостоятельных документах.

7.5.4 В комплект эксплуатационной документации должны входить:

- схема первичного электропитания основных и вспомогательных технических средств ЗИ;
- схема заземления основных и вспомогательных технических средств ЗИ;

- спецификация основных и вспомогательных средств ЗИ;
- спецификация программных средств, установленных в технических средствах ЗИ и в средствах контроля эффективности ЗИ;
- перечень оборудования, подлежащего периодическому контролю, объем и периодичность контрольных проверок;
- формуляр ИС;
- формуляр по ИБ.

7.6 Обеспечение режима ИБ при эксплуатации ИС

В процессе эксплуатации ИС должно быть организовано ограничение доступа к информации, блокирование физических каналов утечки и постоянный контроль реализации политики ИБ, основными направлениями которого являются:
- контроль работы пользователей;
- защита целостности данных и программ;
- управление доступом к приложениям;
- контроль внесения изменений.

7.6.1 Контроль работы пользователей

Контроль работы пользователей включает в себя:
- контроль сетевых подключений к конфиденциальным или критически важным приложениям и контроль полномочий доступа пользователей;
- управление доступом к рабочим местам путем идентификации и аутентификации пользователей, а также, при необходимости, терминала и местонахождение каждого зарегистрированного пользователя;
- ведение журнала учета попыток доступа (успешных и неудачных) к ИС;
- ограничение подключения пользователей в неурочное время;
- контроль процедур поддержания режима ИБ при выборе и использовании паролей;
- контроль оборудования, оставленного без присмотра и его защита от несанкционированного доступа;
- отслеживание времени простоя терминалов в зонах с повышенным риском нарушения ИБ;
- ограничение периода подключения терминала к ИС для пакетной передачи файлов;
- организация разрешительной системы для работы во внеурочное время;
- периодический анализ выходной информации ИС и, при необходимости, контроль удаления лишней информация.

7.6.2 Защита целостности данных и программ от вредоносного программного обеспечения

7.6.2.1 Защита от вирусов:
- организация должна проводить политику, требующую установки только лицензированного программного обеспечения;
- противовирусные программные средства должны регулярно обновляться и использоваться для профилактических проверок (желательно ежедневных);
- необходимо проводить регулярную проверку целостности критически важных программ и данных, наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;
- дискеты и другие сменные носители информации неизвестного происхождения должны проверяться на наличие вирусов до их использования;

- строго придерживаться установленных процедур по уведомлению о случаях поражения ИС компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;

- планирование обеспечения бесперебойной работы организации для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления, особенно для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

7.6.3 Управление доступом к сервисам

7.6.3.1 При использовании электронной почты рекомендуется:

- учитывать уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;

- учитывать возможность неправильной адресации или направления сообщений не по назначению, а также надежность и доступность сервиса в целом.

7.6.3.2 Логический доступ к приложениям предоставляется только зарегистрированным пользователям. Приложения должны:

- контролировать доступ пользователей к данным и приложениям в соответствии с политикой управления доступом, принятой в организации;

- обеспечивать защиту от несанкционированного доступа к системным программам, которые способны обойти средства контроля и обеспечивают возможность НСД;

- не нарушать защиту других систем, с которыми они разделяют информационные ресурсы.

7.6.3.3 Для сведения риска повреждения программного обеспечения к минимуму, необходимо осуществлять жесткий контроль доступа к библиотекам исходных текстов программ. Рекомендуется придерживаться следующих правил:

- не хранить библиотеки исходных текстов программ в ИС;

- распечатки программ хранить в библиотеках исходных текстов;

- ограничивать доступ к библиотекам исходных текстов программ;

- обновление библиотек исходных текстов программ и выдача текстов программ программистам должны производиться только назначенным ответственным сотрудником после получения разрешения в установленной форме на доступ к приложению;

- необходимо фиксировать все случаи доступа к библиотекам исходных текстов программ в контрольном журнале;

- устаревшие версии исходных текстов программ следует архивировать с указанием даты окончания их использования вместе со всем вспомогательным программным обеспечением и информацией об организации выполнения заданий для этой версии программного обеспечения;

- сопровождение и копирование библиотек исходных текстов программ необходимо осуществлять в соответствии с процедурами управления процессом внесения изменений.

Все чрезвычайные ситуации и события, связанные с нарушением режима ИБ, необходимо регистрировать в журнале. Журнал следует хранить в течение заданного промежутка времени. Кроме неудавшихся попыток входа в систему, целесообразно также регистрировать случаи успешного доступа. Контрольный журнал должен включать:

- идентификаторы пользователей;

- дата и время входа и выхода из системы;

- идентификатор или местонахождение терминала (по возможности);

- неудачные попытки доступа в ИС;

- попытки несанкционированного использования восстановленных пользовательских идентификаторов;

- использование ресурсов с привилегированным доступом;
- отдельные действия, потенциально опасные с точки зрения нарушения режима ИБ;
- использование конфиденциальных ресурсов.

7.6.4 Внесение изменений

Внесение изменений в ИС и ее компоненты должно производиться в соответствии с утвержденными процедурами, после обязательной оценки влияния вносимых изменений на режим ИБ.

В необходимых случаях должны быть проведены типовые испытания с целью проверки соответствия характеристик и параметров ИС установленным требованиям после внесения изменений.

Необходимость проведения типовых испытаний определяет разработчик по согласованию с органами надзора (контроля).

Правила доведения внесенных изменений до сведения лиц, которых они затрагивают, должны определяться в инструкциях персоналу в части касающейся непосредственных обязанностей.

Приложение
(справочное)

Библиография

[1] Сборник нормативных правовых актов по защите государственных секретов. – Астана; Агентство по защите государственных секретов, 2002.

[2] Рекомендации ИСО/МЭК 15408-1:2005 Технологии информационные. Методы защиты. Критерии оценки защиты информационных технологий. Часть 1. Введение и общая модель.

[3] Рекомендации ИСО/МЭК 15408-2:2005 Технологии информационные. Методы защиты. Критерии для оценки защиты информационных технологий. Часть 2. Эксплуатационные требования безопасности.

[4] Рекомендации ИСО/МЭК 15408-3:2005 Технологии информационные Методы защиты. Критерии для оценки защиты информационных технологий. Часть 3. Требования к обеспечению защиты.

УДК **МКС 35.240**

Ключевые слова: информационная система, информационная безопасность, средства защиты информации, режим информационной безопасности, стадии и этапы разработки

Для заметок

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

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы, Есіл өзеннің жағалауы, № 35 көше, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074