ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпаратты қорғау

ҚОРҒАЛҒАН ОРЫНДАЛУДАҒЫ АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕЛЕР

Жалпы техникалық талаптар

ҚР СТ 34.024-2006

Ресми басылым

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

Астана

Алғысөз

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

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

3 Осы стандарт Ресей Федерациясы ГОСТ Р 51624-2000 «Ақпаратты қорғау. Қорғалған орындалудағы автоматтандырылған жүйелер. Жалпы ережелер» стандартының негізгі ережелері ескеріліп әзірленген

4 Осы стандартта «Техникалық реттеу туралы», «Қазақстан Республикасындағы тілдер туралы», «Мемлекеттік құпиялар туралы» Қазақстан Республикасы Заңдарының нормалары, Қазақстан Республикасы Ақпараттық қауіпсіздігі тұжырымдамасы, Саудадағы техникалық кедергілер жөніндегі Дүниежүзілік сауда ұйымының Келісімдері іске асырылды

5 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2011 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

6 АЛҒАШ РЕТ ЕНГІЗІЛДІ

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпаратты қорғау
ҚОРҒАЛҒАН ОРЫНДАЛУДАҒЫ АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕЛЕР
Жалпы техникалық талаптар

Енгізілген күні 2008.01.01

1 Қолданылу саласы

Осы стандарт қызметтің барлық түрлерінде (зерттеу, басқару, жобалау және т.б.) құрылуы және қолданылуы процесінде мемлекеттік құпияларға қатысты мәліметтер (бұдан әрі – құпия ақпарат, егер оның құпиялылық дәрежесі ерекше аталмаса) бар қорғалатын ақпаратты өңдеу жүзеге асырылатын олардың үлесімін қоса пайдаланатын қорғалған орындаудағы автоматтандырылған жүйелерге таратылады.

Осы стандарт қорғалған орындаудағы автоматтандырылған жүйелер құру және қолдану бөлігінде «Ақпараттық технология. Автоматтандырылған жүйелерге арналған стандарттар жиынтығы» 34-сыныпты стандарттардың қосымша талаптары мен ережелерін белгілейді.

Осы стандартты Қазақстан Республикасының аумағында мемлекеттік билік, жергілікті өзін-өзі басқару органдары, қорғалған орындаудағы автоматтандырылған жүйелерге тапсырыс беретін, әзірлейтін және пайдаланатын ұйымдастырушылық-құқықтық түрі мен меншік түріне тәуелсіз ұйымдар, кәсіпорындар және мекемелер қолданады.

2 Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтемелер пайдаланылды:

ҚР СТ 34.014-2002 Ақпараттық технология. Автоматтандырылған жүйелерге арналған стандарттардың жиынтығы. Автоматтандырылған жүйелер. Терминдер мен анықтамалар.

ҚР СТ 34.025-2006 Ақпаратты қорғау. Қорғалған орындаудағы автоматтандырылған жүйелерді құру тәртібі. Жалпы ережелер.

ҚР СТ 34.026-2006 Ақпаратты қорғау. Терминдер мен анықтамалар.

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

ҚР СТ ГОСТ Р 50739-2006 Есептегіш техника құралдары. Ақпаратқа санкцияланбаған қол жеткізуден қорғау. Жалпы техникалық ережелер

Ресми басылым

ҚР СТ ГОСТ Р 51275-2006 Ақпаратты қорғау. Ақпараттандыру объектісі. Ақпаратқа әсер ететін факторлар. Жалпы ережелер.

ГОСТ 34.201-89 Ақпараттық технология. Автоматтандырылған жүйелерге арналған стандарттар жиынтығы. Автоматтандырылған жүйелерді құру кезіндегі құжаттардың түрлері, жинақтылығы және белгілері.

ГОСТ 16325-88 Жалпы мақсатқа арналған есептеуіш электронды сандық машиналар. Жалпы техникалық талаптар.

ГОСТ 16504-81 Өнімді мемлекеттік сынау жүйесі. Өнім сапасын сынау және бақылау. Негізгі терминдер мен анықтамалар.

ГОСТ 20397-82 Шағын электрондық есептеуіш машиналардың техникалық құралдары. Жалпы техникалық талаптар, қабылдау ережелері, сынау әдістері, таңбалау, буып-түю, тасымалда және сақтау, әзірлеушінің кепілдігі.

ГОСТ 21552-84 Есептеуіш техника құралдары. Жалпы техникалық талаптар, қабылдау ережелері, сынау әдістері, таңбалау, буып-түю, тасымалда және сақтау, әзірлеушінің кепілдігі.

ГОСТ 23773-88 Жалпы мақсатқа арналған есептеуіш электронды сандық машиналар. Сынау әдістері.

ГОСТ 27201-87 Есептегіш электрондық дербес машиналар. Типтері, негізгі параметрлері, жалпы техникалық талаптар.

ГОСТ 28147-89 Ақпаратты өңдеу жүйесі. Криптографиялық қорғау. Криптогра-фиялық түрлендіру алгоритмі.

3 Терминдер, анықтамалар және қысқартулар

Осы стандартта ҚР СТ 1202 стандартында белгіленген терминдер, сондай-ақ сәйкесті анықтамаларымен бірге мынадай терминдер пайдаланылады:

3.1 **Мемлекеттік құпиялар:** Тиімді әскери, экономикалық, ғылыми-техникалық, сыртқы экономикалық, сыртқы саяси, барлау, контрбарлау, жедел-іздестіру және халықаралық құқықтың [1] жалпы қабылданған ережелеріне қайшы келмейтін, басқа қызметтерді жүзеге асыру мақсатында таралуына мемлекет шек қоятын мемлекеттік және қызметті құпиядан тұратын мемлекет қорғайтын мәліметтер.

3.2 **Құпиялылық белгісі:** Тасушысында бар мәліметтердің құпиялылық дәрежесі туралы куәландыратын, тасушының өзімен және (немесе) оған арналған ілестіру құжаттамасымен жеткізілетін деректемелер.

3.3 **Ақпаратты қорғау:** Жылыстаудан, ұрлануының. жоғалуының, санкциясыз жойылуының, өзгертілуінің, түрлендірілуінің (қолдан жасалуының), санкциясыз көшірілуінің, ақпаратқа берілетін рұқсатқа тосқауыл қоюдың алдын алу мақсатында өткізілетін ұйымдастыру, құқықтық техникалық және технологиялық шаралар [2].

3.4 **Қорғалатын ақпарат:** Меншіктік болып табылатын және құқықтық құжаттардың талаптарына немесе ақпараттың меншік иесі белгілеген қойған талаптарға сәйкес (ҚР СТ 1202 бойынша) қорғалуға жататын ақпарат.

3.5 **Автоматтандырылған жүйе:** Қызметкерлерден және оның қызметін автоматтандыру құралдары жиынтығынан тұратын, белгіленген функцияларды орындайтын ақпараттық технологияны іске асыратын (ҚР СТ 34.014 бойынша) жүйе.

3.6 **Қорғалған орындаудағы автоматтандырылған жүйе:** Белгіленген функцияларды орындайтын ақпараттық технологияны ақпаратты қорғау жөніндегі стандарттардың және/немесе басқа нормативтік құжаттардың талаптарына сәйкес іске асыратын автоматтандырылған жүйе.

3.7 **Біріктірілген автоматтандырылған жүйе:** Екі немесе одан да көп өзара байланысты АҚ жиынтығы, оның ішіндегі біреуінің жұмыс істеуі екіншісінің (басқаларының) жұмыс жасау нәтижелеріне байланысты болғандықтан, осы жиынтықты біртұтас АҚ ретінде қарастыруға болады (ҚР СТ 34.014 бойынша).

3.8 **Автоматтандырылған жүйе ақпаратын қорғау жүйесі:** Ақпаратты қорғаудың барлық техникалық, бағдарламалық және бағдарламалық-техникалық құралдарының және ақпаратты қорғаудың тиімділігін бақылау құралдарының жиынтығы (ҚР СТ 34.025 бойынша).

3.9 **Ақпаратты өңдеу:** Ақпаратты жинау, жинақтау, енгізу, шығару, қабылдау, беру, жазу, сақтау, тіркеу, жою, түрлендіру, бейнелеу операцияларының жиынтығы (ҚР СТ ГОСТ Р 51275 бойынша).

3.10 **Автоматтандырылған жүйені техникалық қамтамасыз ету:** АҚ жұмыс жасап жатқанда пайдаланылатын барлық техникалық құралдардың жиынтығы (ҚР СТ 34.014 бойынша).

3.11 **Автоматтандырылған жүйені бағдарламалық қамтамасыз ету:** АҚ кейінге қалдыруға, жұмыс істеуіне және жұмысқа қабілеттігін тексеруге арналған деректердің және бағдарламалық құжаттардың тасымалдаушысындағы бағдарламалар жиынтығы (ҚР СТ 34.014 бойынша).

3.12 **Сынақтар**: Жұмыс жасауы кезінде, объектіні түрлендіру кезінде оған әсер ететін нәтиже ретінде сынақтардың және/немесе әсерлердің объектісі қасиеттерінің сандық және/немесе сапалық қасиеттерін тәжірибелік анықтау (ГОСТ 16504 бойынша).

3.13 **Қорғалатын ақпаратқа әсер ететін фактор:** Нәтижесінде қорғалатын ақпараттың жария болуы, бұрмалануы, жойылуы, оған берілетін рұқсатқа тосқауыл қою болуы мүмкін құбылыс, іс-әрекет немесе процесс (ҚР СТ ГОСТ Р 51275 бойынша).

3.14 **Ақпарат қауіпсіздігіне төнетін қатер:** Ақпараттың жария болуымен және/немесе санкцияланбаған және/немесе абайсыз оған әсер етумен байланысты әлуетті немесе шынайы бар қауіп төндіретін шарттар мен факторлар жиынтығы.

3.15 **Жанама электромагниттік сәулелену:** Ақпаратты өңдейтін техникалық құралдардың жұмысы барысында пайда болатын электромагниттік сәулелену (ҚР СТ ГОСТ Р 51275 бойынша).

3.16 **Электромагниттік көздеулер (наводкалар):** Ток өткізгіш элементтердегі токтар мен кернеулер, электромагниттік өрістен пайда болған электр зарядтары немесе магниттік ағындар.

3.17 **Салу құрылғы:** Ақпаратты жинап алуға мүмкін бар орындарға (соның ішінде қоршауға, құрастырылымға, жабдыққа, үйдің ішкі көрініс заттарына, көлік құралдарына, сондай-ақ техникалық құралдарға және ақпаратты өңдеу жүйелеріне) жасырын енгізілетін (салынатын немесе енгізілетін) ақпаратты жинап алу құралының элементі (ҚР СТ ГОСТ Р 51275 бойынша).

3.18 **Бағдарламалық салу:** Бағдарламалық қамтамасыз етуге енгізілген атқарымдық объектілер, белгілі бір жағдайларда (кіріс деректері) ақпаратқа санкцияланбаған әсерлерді жүзеге асыруға мүмкіндік беретін, құжаттамада сипатталмаған бағдарламалық қамтамасыз ету қызметтерінің орындалғанын білдіретін, бағдарламалық қамтамасыз етуге енгізілген атқарымдық объектілер (ҚР СТ ГОСТ Р 51275 бойынша).

3.19 **Бағдарламалық вирус:** Санкцияланбаған тарату және өздігінен жаңғыртылу қасиеті бар орындалатын бағдарламалық код немесе нұсқаулардың түсіндірілетін жиынтығы. Таралу процесінде вирустық объектілер өздерін түрлендіре алады. Кейбір бағдарламалық вирустар бағдарламаларды немесе деректерді өзгерте, көшіре немесе жоя алады (ҚР СТ ГОСТ Р 51275 бойынша).

3.20 **Автоматтандырылған жүйенің қорғалу сыныбы:** Автоматтандырылған жүйеге қойылатын ақпаратты қорғау жөніндегі талаптардың белгілі бір жиынтығы.

Осы стандартта мынадай қысқартулар қабылданған:

АЖ - автоматтандырылған жүйе;
ҚОАЖ - қорғалған орындаудағы автоматтандырылған жүйе;
ТТ – техникалық тапсырма;
ҒЗЖ – ғылыми-зерттеу жұмысы;
ТҚЖ - тәжірибелі-құрастырушылық жұмыс;
АҚ – ақпаратты қорғау;
ЖЭМСК - жанама электромагнитті сәулеленулер мен көздеулер;
СНМЕ – санитарлық нормалар мен ережелер;
ҚҚБЖ - құрастырушылық құжаттаманың бірыңғай жүйесі;
ТҚ – техникалық құралдар;
СР – санкцияланбаған рұқсат;
БҚ - бағдарламалық құралдар;
НҚ – нормативтік құжат;

АҚҚ – ақпаратты қорғау құралы;
БҚБЖ – бағдарламалық құжаттаманың бірыңғай жүйесі;
ТҚБЖ – технологиялық құжаттаманың бірыңғай жүйесі.

4 Жалпы ережелер

4.1 ҚОАЖ жобалау, жасау және пайдалану ақпаратты қорғау жөніндегі нормативтік құжаттардың талаптары, осы стандарттың, ақпаратты қорғау жөніндегі талаптары бөлігінде АЖ арналған стандарттар мен техникалық тапсырманың талаптары есебімен жүзеге асырылуға тиіс.

ҚОАЖ-де мемлекеттік құпияларды құрайтын мәліметтерден тұратын ақпаратты қорғауға арналған шифрлау техникасын пайдалану тәртібі қолданыстағы НҚ талаптарына сәйкес анықталады.

4.2 ҚОАЖ пайдаланушыға қорғалған өнім түрінде жеткізуге және әзірлеуге рұқсат етіледі. Қорғалатын ақпаратты өңдеуге арналған жұмыс істейтін (пайдаланылатын) және түрлендірілетін АҚ ақпаратты қорғаудың қосымша жүйемен қамтамасыз етілуге тиіс.

4.3 Ақпаратты қорғау жөніндегі талаптарды тұтастай ҚОАЖ да, сол сияқты қажет болса құрама құрамбөліктерге де (бөлімдеріне) тапсыру беруші белгілейді.

ҚОАЖ құрамбөліктеріне (құрама бөліктеріне) қойылатын ақпаратты қорғау жөніндегі талаптар тұтасымен жүйенің ақпаратты қорғау жөніндегі талаптармен келісілуге тиіс.

4.4 Ақпаратты қорғау жөніндегі ҚОАЖ қойылатын талаптар «Ақпаратты қорғау жөніндегі талаптар» ҒЗЖ (ТКЖ)-ға жеке бөлімшесі түрінде жүйе құруға ТТ-да беріледі.

Қажет болса ҚОАЖ жасауға ТТ-да немесе оның құрам бөліктеріне тапсырыс беруші ақпаратты қорғау жөнінде осы стандарт талаптарын толықтыратын және анықтайтын ерекше талаптар кіргізе алады.

ҚОАЖ техникалық немесе эскиздық жобалау нәтижелері бойынша, қажетіне қарай, бекітілген ТТ-ға өзгерістер енгізу үшін белгіленген тәртіппен түзетуге рұқсат етіледі.

4.5 ҚОАЖ-де ақпаратты қорғау:

- ҚОАЖ-де ақпаратты қорғаудың нақты мақсатын іске асыру мүддесінде жүзеге асырылатын, мақсатқа сай;
- ҚОАЖ құрастырылымдық элементтерінің барлық көптүрлілігін ҚОАЖ үшін қауіп-қатердің барлық спектрінен қорғау мүдделерінде жүзеге асырылатын жинақтық;
- өңделетін ақпараттың маңыздылығына, ҚОАЖ ресурстарының күйіне, ақпаратты қорғау қауіп-қатерліктерді қадағалау нәтижелерінің ҚОАЖ пайдалану жағдайларына байланысты ҚОАЖ өмірлік циклінің барлық кезеңінде жүзеге асырылатын басқарылатын;

- ақпаратты қорғау әдістері мен құралдары ақпаратты қорғаудың қажетті деңгейін техникалық арналар, ақпаратқа рұқсатсыз қол жеткізу, беру түріне тәуелсіз оған рұқсатсыз және абайсызда әсер ету жөніндегі жария болудан қорғауды қамтамасыз етуге тиіс, кепілді болуға тиіс.

4.6 ҚОАЖ-де ақпаратты қорғау жүйесі іске асырылуға тиіс, ол мынадай жұмыстар атқарады:

- ақпарат қауіпсіздігі қатері пайда болғаны туралы сақтандыру;
- ақпарат қауіпсіздігі қатерін табу, бейтараптау және оқшаулау;
- қорғалатын ақпаратқа рұқсатты басқару;
- қауіп-қатерлер әсер етуден кейін ақпаратты қорғау жүйені және қорғалатын ақпаратты қалпына келтіру;
- қорғалатын ақпаратқа санкцияланбаған рұқсат және оған санкцияланбаған әсер ету оқиғалары мен ұмтылыстарын тіркеу;
- ақпаратты қорғау құралдары мен жүйелерінің жұмысын бақылауды қамтамасыз ету және олардың істен шығуына дереу әрекет ету.

4.7 ҚОАЖ әзірлеу (түрлендіру) және пайдалану кезінде әзірлеушілердің, пайдаланушылардың, пайдаланушы қызметкерлердің техникалық және бағдарламалық құралдарға, сондай-ақ ҚОАЖ ақпараттық ресурстарына қол жеткізуге рұқсат беру жүйесі ұйымдастырылуға тиіс.

Пайдаланушыларға өздеріне белгіленген атқарымдық міндеттерді орындау үшін қажетті құралдармен және ресурстармен ғана жұмыс істеу құқығы беріледі.

ҚОАЖ ресурстарына рұқсат алу жөніндегі әзірлеушілердің, пайдаланушылардың және пайладанушы қызметкерлердің өкілеттіктерін жүйеге тапсырыс беруші белгілейді және «Орындаушылардың кәсіпорындағы құжаттарға және мәліметтерге қол жеткізуіне рұқсат беру жүйесі туралы ережелер» бөлімінде және ҚОАЖ пайдалану жөніндегі нұсқаулықтарда ҚОАЖ құруға (түрлендіруге) ТТ-да бейнеленеді.

4.8 ҚОАЖ-де мыналар:

- қорғалатын ақпараты бар ақпараттық жиындар және дерекқор түріндегі және магниттік, оптикалық және басқа тасымалдаушылармен берілген ақпараттық ресурстар;
- автоматтандыру құралдары (есептегіш техника құралдары, ақпараттық-есептеу жиынтықтар, желілер және жүйелер), бағдарламалық құралдар (амалдық жүйелер, дерекқорларды басқару жүйелері, басқа жалпыжүйелік және қолданбалы бағдарламалық қамтамасыз ету), басқарудың автоматтандырылған жүйелері, байланыс және деректер беру жүйелері және басқа құралдар қорғалуға тиіс.

4.9 ҚОАЖ-де ақпаратты қорғау жүйесі құрылатын ҚОАЖ ажыратылмас құрама бөлігі болып табылады немесе түрлендірілген жұмыс жасаушы автоматтандырылған жүйенің қосымша ішкі жүйесі түрінде жүзеге

асырылады. ҚОАЖ ақпаратты қорғау жүйесіне қойылатын талаптар қолданыстағы нормативтік құжаттарға сәйкес беріледі.

5 Жалпы талаптар

5.1 ҚОАЖ қойылатын жалпы талаптарға:
- атқарымдық талаптар;
- тиімділікке қойылатын талаптар;
- техникалық талаптар;
- экономикалық талаптар;
- құжаттамаға қойылатын талаптар кіреді.

5.2 ҚОАЖ қойылатын атқарымдық талаптарға талаптардың мынадай топтары:
- ҚОАЖ өңделетін ақпараттың құпиялық (жасырын) белгілері;
- ҚОАЖ қорғалу сыныбы;
- ақпаратты қорғау мақсаттары;
- ҚОАЖ қорғалатын ақпараттың тізімі және оны қорғау тиімділігінің талап етілетін деңгейлері;
- ақпараттың кетуінің ықтимал техникалық арналары және ақпаратқа санкцияланбаған қол жеткізу тәсілдері, ҚОАЖ ақпаратқа санкцияланбаған және абайсызда әсерлер ету тәсілдері, ҚОАЖ қорғалу сыныбы кіреді.

5.2.1 Ақпараттың құпиялық (жасырын) белгісін, ҚОАЖ қорғау санаттарын анықтауды ақпаратты қорғау саласындағы қолданыстағы басқарушы және нормативтік құжаттарға сәйкес тапсырыс беруші жүзеге асырады.

5.2.2 ҚОАЖ қорғалу тобын анықтау қолданыстағы нормативтік құжаттарға сәйкес жүзеге асырылады.

5.2.3 ҚОАЖ-де ақпаратты қорғау мақсаттары

5.2.3.1 ҚОАЖ-де АҚ жалпы мақсаты осы жүйенің иесіне және/немесе оны пайдаланушыға ақпарат қауіпсіздігі қауіп-қатерін іске асыру салдарынан тиген зиянның алдын алу немесе көлемін азайту болып табылады.

Ақпаратты қорғаудың ҚОАЖ жалпы мақсатына қол жеткізуді қамтамасыз ететін жеке мақсаттары:
- техникалық арналар бойынша ақпараттың жария болуының алдын алу;
- ақпаратты санкцияланбаған жоюдың, бұрмалаудың, көшірудің, бұғаттаудың алдын алу;
- жиымдарды, ақпаратты өңдеу бағдарламаларын пайдаланудың, өңдеу жүйелерінде ақпараттың толықтығын, тұтастығын, растығын қамтамасыз етудің құқықтық режімін сақтау;
- өңдеу процесін басқару және қорғалатын ақпаратқа санкцияланбаған әсер ету жағдайларында ақпаратты пайдалау мүмкіндігін сақтау.

5.2.3.2 ҚОАЖ-де ақпаратты қорғау мақсаттарына:

- қорғау мақсатының маңызды түсіндірмесі;
- мақсатқа қол жеткізу тиімділігінің көрсеткіші және оның талап етілетін мәні;
- ақпаратты қорғаудың әрбір мақсатының өзектілік уақыты (мақсатқа қол жеткізілуге тиісті өмірлік циклдың кезеңдері).

5.2.4 ҚОАЖ-дегі ақпаратты қорғаудың әрбір міндетінің түсіндірмесіне:

- міндеттерді шешу кезінде алдын алу (жою) қажет ҚОАЖ (оның құрамбөлігі) үшін қауіпсіздіктің нақты қауіп-қатерінің атауы;
- міндетті шешу тәсілінің түсіндірмесі;
- осы міндетті шешу үшін іске асырылуға тиісті функциялардың тізбесі;
- міндетті шешу тиімділігіне немесе кепілділіктеріне қойылатын талаптар;
- осы міндетті шешуге бөлінген ҚОАЖ ресурстарына шектеулер кіреді.

5.2.4.1 ҚОАЖ-де ақпаратты қорғау міндеттеріне:

- байланыс арналары бойынша берілетін қорғалатын ақпаратты алып қоюдың алдын алу;
- жанама электромагниттік сәулелену және көздеу есебінен өңделетін қорғалатын ақпараттың жария болуының алдын алу;
- өңделетін немесе ҚОАЖ-де сақталатын қорғалатын ақпаратқа санкцияланбаған қол жеткізуді жою;
- қорғалатын ақпаратты бұзатын, жоятын, бұрмалайтын санкцияланбаған және абайсызда жасалатын әсерлердің және ҚОАЖ құралдарының жұмысындағы жаңылысудың алдын алу;
- ҚОАЖ техникалық құралдарына ықтимал енгізілген ақпаратты ұстайтын арнайы электрондық құрылғыларды табу;
- ҚОАЖ-дегі қорғау құралдары мен жүйелерінің жұмыс істеуіне бақылау жасау кіреді.

5.2.5 ҚОАЖ-де қорғалатын ақпараттың тізбесі және оны қорғау тиімділігінің талап етілетін нормалары (деңгейлері).

5.2.5.1 ҚОАЖ-де қорғалатын ақпараттың нақты тізбесін анықтау ҚОАЖ тағайындалуына, ақпаратты қорғау мақсаттарына, ҚОАЖ құрамы мен құрылымына, сондай-ақ ақпаратты қорғау құрамы мен құрылымына сүйеніп жүзеге асырылуға тиіс.қорғалатын ақпараттың тізбесі тұтасымен ҚОАЖ үшін де, сондай-ақ оның құрама бөліктері (құрамбөліктері) үшін де анықталады.

5.2.5.2 ҚОАЖ-де ақпаратты қорғау тиімділігі жөніндегі талаптарға:

- ақпаратты қорғаудың іске асырылатын тәсілдерінің тізбесі;
- ақпаратты қорғау тиімділігінің көрсеткіштерінің тізбесі;
- ақпаратты қорғау тиімділігінің талап етілетін деңгейлері кіруге тиіс.

5.2.6 ҚОАЖ-де ақпараттың жария болуының ықтимал техникалық арналарын, санкцияланбаған рұқсатты, оған тиетін санкцияланбаған және

абайсызда әсер етуді анықтау ҚОАЖ құрамын, құрылымын, жұмыс істеу алгоритмін талдау, ҚОАЖ ақпаратты қорғау қауіп-қатерлер үлгілерін пайдалана отырып орналастыру шарттары, қолданыстағы нормативтік құжаттарға сәйкес ақпаратқа әсер ететін факторларды атаутізімі негізінде жүзеге асырылуға тиіс.

Ақпараттың жария болуын техникалық арналарының қауіптілігін, ақпаратқа санкцияланбаған рұқсаттың ықтимал тәсілдерін және оған тиетін санкцияланбаған әсерлерді бағалау тиісті жұмыстар өткізуге арналған уәкілетті мемлекеттік органның нормативтік және әдістемелік құжаттарында анықталған көрсеткіштер мен әдістемелер бойынша жүзеге асырылады.

5.3 ҚОАЖ-де ақпаратты қорғау міндеттерін шешудің тиімділігіне немесе кепілдіктеріне қойылатын талаптарға:

- техникалық арналар бойынша қорғалатын ақпараттың жария болуының алдын алу жөніндегі талаптар;
- қорғалатын ақпаратқа санкцияланбаған рұқсаттың алдын алу жөніндегі талаптар;
- ақпаратты бұзатын, жоятын, бұрмалайтын немесе ҚОАЖ құралдарының жұмысында жаңылысу тудыратын санкцияланбаған және абайсызда болған әсерлердің алдын алу жөніндегі талаптар;
- үй-жайларға және техникалық құралдарға енгізілген ақпаратты ұстайтын арнайы электрондық құралдарды табу жөніндегі талаптар;
- ҚОАЖ ақпаратын қорғау жүйесінің жұмыс жасауына бақылау жөніндегі талаптар кіреді.

5.3.1 Техникалық арналар бойынша қорғалатын ақпараттың жария болуының алдын алу жөніндегі талаптар

5.3.1.1 Қорғалатын ақпараттың жария болуының алдын алу жөніндегі талаптарға:

- жанама электромагниттік сәулелену және көздеулер есебінен қорғалатын ақпараттың жария болуының алдын алу жөніндегі талаптар;
- барлаудың техникалық арналары бойынша қорғалатын ақпараттың жария болуының алдын алу жөніндегі талаптар;
- жүйенің жұмыс істеуін қамтамасыз ететін АҚ техникалық құралдарынан сәулеленіп бөлінетін сигналдар есебінен қорғалатын ақпараттың жария болуының алдын алу жөніндегі талаптар;
- қорғалатын ақпаратқа санкцияланбаған рұқсаттың есебінен оның жария болуының алдын алу жөніндегі талаптар кіреді.

5.3.1.2 ҚОАЖ құрамына кіретін және қорғалуға тиіс есептегіш техника құралдары жанама электромагниттік сәулелену және көздеулер есебінен жария болудан ақпаратты қорғау жөніндегі талаптарды қанағаттандыруға тиіс. Жанама электромагниттік сәулелену және көздеулер есебінен жария болудан ақпаратты қорғау тиімділігінің көрсеткіштерінің атаутізімі қолданыстағы нормативтік құжаттарға сәйкес анықталады.

5.3.1.3 Барлаудың техникалық арналары бойынша қорғалатын ақпараттың жария болуының алдын алу талаптарына:

- техникалық барлау арналары бойынша қорғалатын ақпараттың жария болуының алдын алу жөніндегі талаптар;
- техникалық құралдарды пайдаланатын агенттік барлау арналары бойынша қорғалатын ақпараттың жария болуының алдын алу жөніндегі талаптар кіреді.

Техникалық және агенттік барлау арналары бойынша қорғалатын ақпараттың жария болуының алдын алу жөніндегі талаптар қолданыстағы нормативтік құжаттарға сәйкес белгіленеді.

5.3.1.4 ҚОАЖ құрылымдық құрамбөліктерінің жұмыс істеуінің ақпаратқа әсер ететін сыртқы факторларға төзімділігі жөніндегі талаптар ГОСТ 16325, ГОСТ 20397, ГОСТ 21552, ГОСТ 27201 бойынша ҚОАЖ құрамбөліктерінің нақты сыныптарына (түрлеріне, типтеріне) белгіленеді.

ҚОАЖ-нің ақпаратқа ішкі әсер ету факторларына (істен шығу, жаңылысу, қателер) төзімділігі жөніндегі талаптар нақты жүйенің немесе оның құрамбөліктерінің жұмыс жасау сенімділігі мен тұрақтылығы талаптарымен бірге және ГОСТ 20397, ГОСТ 16325, ГОСТ 21552, ГОСТ 27201 бойынша белгіленеді.

5.3.1.5 ҚОАЖ-де кірістірілген электрондық және/немесе бағдарламалық тыңшы құрылғылары арқылы жария болуын алдын алу жөніндегі талаптарға ішіне орнатылған салу құрылғыларын анықтау және оларды жою жөніндегі кіреді. Осы талаптар қолданыстағы басшылық және нормативтік құжаттарға сәйкес белгіленеді.

5.3.2 Қорғалатын ақпаратқа санкцияланбаған рұқсаттың алдын алу жөніндегі талаптар ҚР СТ ГОСТ Р 50739 бойынша және уәкілетті мемлекеттік органның нормативтік құжаттары бойынша белгіленеді.

5.3.3 Ақпаратты бұзатын, жоятын, бұрмалайтын немесе ҚОАЖ ақпарат құралдарының жұмысы барысында жаңылыстыратын санкцияланбаған және абайсызда жасалған әсерлердің алдын алу жөніндегі талаптар ақпаратты қорғау саласындағы қолданыстағы құқықтық, басшылық және нормативтік құжаттарға сәйкес белгіленеді.

ҚОАЖ-ге сырттан әсер ететін факторлар есебінен ақпараттың өзгеруінің алдын алу жөніндегі талаптар ГОСТ 20397, ГОСТ 21552, ГОСТ 27201 бойынша ҚОАЖ құрамбөліктеріне қойылатын талаптар есебімен белгіленеді.

Сыртқы жанама құбылыстар (электромагниттік өрістер) есебінен ақпараттың өзгеруінің алдын алу жөніндегі талаптар электромагниттік сыйымдылық жөніндегі нормаларға және қолданыстағы нормативтік құжаттарға сәйкес белгіленеді.

ҚОАЖ-де комьютерлік вирустарды қосатын қаскүнемнің субъективті қасақана жасаған әрекеттері есебінен қорғалатын ақпараттың өзгертуінің

алдын алу жөніндегі талаптар қолданыстағы нормативтік құжаттарға сәйкес белгіленеді және арнайы бағдарламалық және аппараттық қорғау құралдарын (вирустарға қарсы бағдарламалар) қолдану арқылы және бағдарламалық қамтамасыз етудің қауіпсіздігін бақылау жүйесін ұйымдастыру арқылы қол жеткізіледі.

5.4 Ақпаратты қорғау жөніндегі техникалық талаптарға ҚОАЖ қамтамасыз етудің негізгі түрлеріне:

- техникалық және бағдарламалық;

- ҚОАЖ орнатылатын ғимараттарға (үй-жайларға) немесе объектілерге, сондай-ақ ақпаратты қорғау және ақпаратты қорғау тиімділігін бақылау құралдарына қойылатын талаптар кіреді.

5.4.1 ҚОАЖ техникалық қамтамасыз етуге қойылатын ақпаратты қорғау жөніндегі талаптарға ҚОАЖ атқарымдық тағайындау бойынша пайдаланылатын негізгі техникалық құралдарға қойылатын талаптар да, сол сияқты негізгі техникалық құралдардың жұмыс жасауын қамтамасыз ететін көмекші техникалық құралдарға қойылатын талаптар да кіреді.

5.4.1.1 Негізгі техникалық құралдарға қойылатын техникалық талаптарда ЖЭМСК бойынша жария болудан, салу құрылғыларынан, сыртқы және ішкі әсер етуші факторлардан, ақпаратқа санкцияланбаған рұқсаттан және оған санкцияланбаған әсер етуден ақпаратты қорғау талаптары болады.

5.4.1.2 АҚ техникалық құралдарына қойылатын құрастырылымдық талаптар ақпаратты қорғау жөніндегі талаптарды есебінен құрылуға және ҚОАЖ нақты техникалық құралын әзірлеуге арналған ТТ «Құрастырылымдық талаптар» бөліміне кіруге тиіс.

5.4.1.3 ҚОАЖ техникалық құралдары электрмен қоректендіру ажыратылған жағдайда, апат болғанда, сондай-ақ табиғаттың қолайсыз құбылыстары және стихиялық апаттар жағдайларында ақпараттың сақталуы қамтамасыз етілуге тиіс.

5.4.1.4 ҚОАЖ техникалық құралдарды бақылау, сынау және қабылдау әдістері ГОСТ 23773 сәйкес келуге тиіс.

5.4.1.5 ҚОАЖ жерге қосу жүйесіне және электрмен қоректендіру желісіне қойылатын талаптар сәйкесті нормативтік құжаттардың талаптарына сәйкес белгіленуге тиіс.

5.4.2 Телекоммуникациялар желісін (деректер беру желісін) қорғауға қойылатын талаптар тиісті нормативтік құжаттардың талаптарына сәйкес белгіленеді.

5.4.3 ҚОАЖ бағдарламалық қамтамасыз етуге қойылатын ақпаратты қорғау жөніндегі талаптар ақпаратты қорғау саласында қолданыстағы басшылық және нормативтік құжаттарға сәйкес регламенттеледі.

5.4.4 ҚОАЖ орнатылатын ғимараттарға (үй-жайларға) немесе құрылғыларға қойылатын АҚ жөніндегі талаптарға ғимараттың (үй-жайдың)

қоршайтын құрылымдарына, құрылыс технологиясына қойылатын талаптар, коммуникациялар құралдарына қойылатын талаптар және үй-жайлардың дыбыс өткізбеуіне қойылатын талаптар кіреді.

5.4.4.1 ҚОАЖ орналасатын объектінің үй-жайларын және құрылыстарын қайта құру немесе кеңейту қажет болған жағдайда ақпаратты қорғау жөніндегі талаптар СНМЕ-ге және басқа қолданыстағы басшылық және нормативтік құжаттарға сәйкес қойылады.

5.4.4.2 ҚОАЖ негізгі техникалық құралдарын құпия (жасырын) келіссөздер жүргізуге арналған үй-жайларға орналастыру кезінде ҚОАЖ негізгі және көмекші техникалық құралдарына акустоэлектрикалық түрлендірулер есебінен сөйлеу ақпаратының жайылып кетуінен қорғау жөнінде шаралар қабылдануға тиіс.

5.4.5 Ақпаратты қорғау құралдарына және ақпаратты қорғаудың тиімділігін бақылау құралдарына қойылатын талаптар

5.4.5.1 Ақпаратты қорғау және ақпаратты қорғаудың тиімділігін бақылау құралдарына қойылатын талаптардың атаутізімі және мазмұны қолданыстағы нормативтік құжаттарға және ақпаратты қорғау және оның тиімділігін бақылау құралдарына арналған техникалық шарттарға сәйкес анықталады.

5.4.6 Ақпаратты қорғау міндеттерін шешуге бөлінетін ҚОАЖ аппараттық, бағдарламалық, ақпараттық, уақытша және басқа ресурстарға шектеулер негізгі атқарымдық тағайындалуы бойынша ҚОАЖ жұмыс жасау тиімділігін рұқсат етілетін төмендетуге сүйене отырып ҚОАЖ бар ресурстарының есебімен анықтайды.

5.5 АҚ жөніндегі экономикалық талаптарға:

- ҚОАЖ және/немесе ҚОАЖ-де ақпаратты қорғау жүйесін құруға тапсырыс беретін ұйымдар үшін рұқсат етілетін шығындар;
- ҚОАЖ және/немесе ҚОАЖ-де ақпаратты қорғау жүйесін пайдаланатын ұйымдар үшін рұқсат етілетін шығындар кіреді.

5.6 ҚОАЖ арналған құжаттамаға қойылатын талаптар

5.6.1 ҚОАЖ арналған құжаттаманың жиынтығы нормативтік құжаттарда және ГОСТ 34.201 бойынша белгіленеді және қосымша 1-кестеде көрсетілген құжаттар кіреді.

5.6.2 Ақпаратты қорғау және оның тиімділігін бақылау құралдарына арналған құрастырылымдық, технологиялық пен пайдалану құжаттамасының жиынтығына қойылатын талаптар

Техникалық құралдарға ҚҚБЖ талаптарына сәйкес құрастырылымдық және пайдалану құжаттамасы әзірленеді.

1-кесте - Автоматтандырылған жүйеге арналған ақпаратты қорғау жөніндегі қосымша құжаттаманың атаутізімі

Құжат атауы	ГОСТ 34.201 бойынша құжаттың коды	Ескерту
1 ҚОАЖ негізгі және көмекші техникалық құралдарының алғашқы электрмен қорек-тендіру сұлбасы	С7*	АҚ бойынша талаптар есебімен
2 ҚОАЖ негізгі және көмекші техникалық құралдарының жерге қосу сұлбасы	С7*	АҚ бойынша талаптар есебімен
3 ҚОАЖ негізгі және көмекші техникалық құралдарының, бағдарламалық құралдарының спецификациясы	-	
4 Режімдік мәселелер бойынша ҚОАЖ (желі) абоненттеріне арналған басшылық	ПН4	АҚ бойынша талаптар есебімен
5 ҚОАЖ қорғалғанын растау жөніндегі бақылау сынақтарының және тексеріс-терінің тізбесі (көлемі және кезеңділігі)	-	
6 ТҚ пайдалануға нұсқау	Д130	АҚ бойынша талаптар есебімен
7 Сәйкестік сертификаты (әрбір жүйенің және АҚҚ, ТТ, БҚ)	-	
8 ҚОАЖ құралдарын және ақпаратты қорғау мәселелері жөніндегі жүйені тұтасымен санаттау актісі	-	
9 Жүйедегі ақпаратқа РЕ-ден қорғау бөлігінде ҚОАЖ жіктеу актісі	-	
10 ҚОАЖ-нің ақпаратты қорғау жөніндегі НҚ талаптарына сәйкестігін растайтын құжат	-	
11 Ақпаратты қорғау жөніндегі формуляр (техникалық паспорт)	-	
12 Тұжырымдамалар, ережелер, басшылықтар, нұсқаулар, нұсқаулық-тар, жарғылар, ережелер, нормалар, үлгілер	-	
*Коды ҚҚБЖ стандарттарының талаптарына сәйкес белгіленген құжаттар		

Бағдарламалық құралдарға БҚБЖ сәйкес құрастырылымдық және пайдалану құжаттамасы әзірленеді.

Бағдарламалық-техникалық құралдарға БҚБЖ, ҚҚБЖ, ТҚБЖ талаптарына сәйкес құрастырылымдық және пайдалану құжаттамасы әзірленеді.

5.6.3 Құжаттардың құрамына, түрлеріне қойылатын және ұйымдастыру-басқару құжаттамасының мазмұнына қойылатын талаптар қолданыстағы басшылық пен нормативтік құжаттарға сәйкес белгіленеді.

Қосымша
(анықтамалық)

Библиография

[1] Қазақстан Республикасының Заңы	«Мемлекеттік құпиялар туралы»
[2]	ҚР Президент жарлығы бекіткен 10.10.2006 №199 Қазақстан Республикасы ақпараттық қауіпсіздігінің тұжырымдамасы

ӘОС681.3 **МСЖ 35.040**

Түйінді сөздер: қорғалатын ақпарат, автоматтандырылған жүйе, қорғалған орындаудағы автоматтандырылған жүйе, ақпаратты қорғау жөніндегі талаптар, ақпаратты қорғау құралдары, ақпаратты қорғау тиімділігін бақылау құралдары, ақпаратты қорғау жүйесі, ақпаратты қорғау құралдарын сертификаттау, ақпаратты қорғау тиімділігін бақылау.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Защита информации

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Общие технические требования

СТ РК 34.024-2006

Издание официальное

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

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 от 15 декабря 2006 г. № 550

3 Настоящий стандарт разработан с учетом основных положений стандарта Российской Федерации ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения**».**

4 В настоящем стандарте реализованы нормы законов Республики Казахстан О техническом регулировании, О языках в Республике Казахстан, О государственных секретах, Концепция информационной безопасности Республики Казахстан, Соглашения Всемирной торговой организации по техническим барьерам в торговле.

5 СРОК ПЕРВОЙ ПРОВЕРКИ 2011 г.
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

6 ВВЕДЕН ВПЕРВЫЕ

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Защита информации

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Общие технические требования

Дата введения 2008.01.01

1 Область применения

Настоящий стандарт распространяется на автоматизированные системы в защищенном исполнении, используемые в различных видах деятельности (исследования, управление, проектирование, производство и т. п.), включая их сочетания, в процессе создания и применения которых осуществляется обработка защищаемой информации, содержащей сведения, отнесенные к государственным секретам (далее – секретная информация, если степень ее секретности не оговаривается особо).

Настоящий стандарт устанавливает дополнительные требования и положения стандартов класса 34 "Информационная технология. Комплекс стандартов на автоматизированные системы" в части создания и применения автоматизированных систем в защищенном исполнении.

Настоящий стандарт применяется на территории Республики Казахстан органами государственной власти, местного самоуправления, организациями, предприятиями и учреждениями независимо от их организационно-правовой формы и формы собственности, которые заказывают, разрабатывают, производят и эксплуатируют автоматизированные системы в защищенном исполнении.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК 34.014-2002 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

СТ РК 34.025-2006 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

СТ РК 34.026-2006 Защита информации. Термины и определения.

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

СТ РК ГОСТ Р 50739-2006 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

СТ РК ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.

ГОСТ 16325-88 Машины вычислительные электронные цифровые общего назначения. Общие технические требования.

Издание официальное

ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения.

ГОСТ 20397-82 Средства технические малых электронных вычислительных машин. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение, гарантия изготовителя.

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

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

ГОСТ 27201-87 Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования.

ГОСТ 28147-89 Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

3 Термины, определения и сокращения

В настоящем стандарте применяют термины, установленные в СТ РК 1202, а также следующие термины с соответствующими определениями:

3.1 **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 [1].

3.2 **Гриф секретности:** Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него [1].

3.3 **Защита информации**: Организационные, правовые технические и технологические мероприятия, проводимые в целях предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования доступа к информации [2].

3.4 **Защищаемая информация**: Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (по СТ РК 1202).

3.5 **Автоматизированная система** - Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (по СТ РК 34.014).

3.6 **Автоматизированная система в защищенном исполнении**: Автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или иных нормативных документов по защите информации.

3.7 **Интегрированная автоматизированная система**: Совокупность двух или более взаимоувязанных АС, в которой функционирование одной из них зависит от результатов функционирования другой (других) так, что эту совокупность можно рассматривать как единую АС (по СТ РК 34.014).

3.8 **Система защиты информации автоматизированной системы**: Совокупность всех технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации (по СТ РК 34.025).

3.9 **Обработка информации**: Совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения информации (по СТ РК ГОСТ Р 51275).

3.10 **Техническое обеспечение автоматизированной системы**: Совокупность всех технических средств, используемых при функционировании АС (по СТ РК 34.014).

3.11 **Программное обеспечение автоматизированной системы:** Совокупность программ на носителях данных и программных документов, предназначенных для отладки, функционирования и проверки работоспособности АС (по СТ РК 34.014).

3.12 **Испытания:** Экспериментальное определение количественных и/или качественных характеристик свойств объекта испытаний как результата воздействия на него при его функционировании, при моделировании объекта и/или воздействий (по ГОСТ 16504).

3.13 **Фактор, воздействующий на защищаемую информацию**,: Явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней (по СТ РК ГОСТ Р 51275).

3.14 **Угроза безопасности информации**: Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на нее.

3.15 **Побочное электромагнитное излучение**: Электромагнитное излучение, возникающее при работе технических средств обработки информации (по СТ РК ГОСТ Р 51275).

3.16 **Электромагнитные наводки**: Токи и напряжения в токопроводящих элементах, электрические заряды или магнитные потоки, вызванные электромагнитным полем.

3.17 **Закладное устройство**: Элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации) (по СТ РК ГОСТ Р 51275).

3.18 **Программная закладка**: Внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций программного обеспечения, позволяющих осуществлять несанкционированные воздействия на информацию (по СТ РК ГОСТ Р 51275).

3.19 **Программный вирус**: Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойством несанкционированного распространения и самовоспроизведения (репликации). в процессе распространения вирусные объекты могут себя модифицировать. Некоторые программные вирусы могут изменять, копировать или удалять программы или данные (по СТ РК ГОСТ Р 51275).

3.20 **Класс защищенности автоматизированной системы**: Определенная совокупность требований по защите информации, предъявляемых к автоматизированной системе.

В настоящем стандарте приняты следующие сокращения:

АС - автоматизированная система;

АСЗИ - автоматизированная система в защищенном исполнении;

ТЗ - техническое задание;

НИР - научно-исследовательская работа;

ОКР - опытно-конструкторская работа;

ЗИ - защита информации;

ПЭМИН - побочные электромагнитные излучения и наводки;

СаНПиН - санитарные нормы и правила;

ЕСКД - единая система конструкторской документации;
ТС - технические средства;
НСД - несанкционированный доступ;
ПС - программные средства;
НД - нормативный документ;
СрЗИ - средство защиты информации;
ЕСПД - единая система программной документации;
ЕСТД - единая система технологической документации.

4 Общие положения

4.1 Проектирование, производство и эксплуатация АСЗИ должны осуществляться с учетом требований нормативных документов по защите информации, требований настоящего стандарта, стандартов и/или технического задания на АС в части требований по защите информации.

Порядок использования в АСЗИ шифровальной техники, предназначенной для защиты информации, содержащей сведения, составляющие государственные секреты, определяется в соответствии с требованиями действующих НД.

4.2 АСЗИ допускается разрабатывать и поставлять потребителю в виде защищенного изделия. Функционирующие (эксплуатируемые) и модернизируемые АС, предназначенные для обработки защищаемой информации, должны обеспечиваться дополнительной системой защиты информации.

4.3 Требования по защите информации устанавливаются заказчиком как на АСЗИ в целом, так при необходимости и на составные компоненты (части).

Требования по защите информации, предъявляемые к компонентам (составным частям) АСЗИ должны быть согласованы с требованиями по защите информации системы в целом.

4.4 Требования по защите информации, предъявляемые к АСЗИ, задаются в ТЗ на создание системы в виде отдельного подраздела ТЗ на НИР (ОКР) "Требования по защите информации".

При необходимости в ТЗ на создание АСЗИ или в его составные части заказчик может включать специфические требования по защите информации, дополняющие или уточняющие требования настоящего стандарта.

По результатам технического и эскизного проектирования АСЗИ требования по защите информации, при необходимости, допускается корректировать в порядке, установленном для внесения изменений в утвержденное ТЗ.

4.5 Защита информации в АСЗИ должна быть:

- целенаправленной, осуществляемой в интересах реализации конкретной цели защиты информации в АСЗИ;
- комплексной, осуществляемой в интересах защиты всего многообразия структурных элементов АСЗИ от всего спектра опасных для АСЗИ угроз;
- управляемой, осуществляемой на всех стадиях жизненного цикла АСЗИ, в зависимости от важности обрабатываемой информации, состояния ресурсов АСЗИ, условий эксплуатации АСЗИ результатов отслеживания угроз безопасности информации;
- гарантированной: методы и средства защиты информации должны обеспечивать требуемый уровень защиты информации от ее утечки по техническим каналам, несанкционированного доступа к информации, несанкционированным и непреднамеренным воздействиям на нее, независимо от форм ее представления.

4.6 В АСЗИ должна быть реализована система защиты информации, выполняющая следующие функции:

- предупреждение о появлении угроз безопасности информации;
- обнаружение, нейтрализацию и локализацию воздействия угроз безопасности информации;
- управление доступом к защищаемой информации;
- восстановление системы защиты информации и защищаемой информации после воздействия угроз;
- регистрацию событий и попыток несанкционированного доступа к защищаемой информации и несанкционированного воздействия на нее;
- обеспечение контроля функционирования средств и системы защиты информации и немедленное реагирование на их выход из строя.

4.7 При разработке (модернизации) и эксплуатации АСЗИ должна быть организована разрешительная система доступа разработчиков, пользователей, эксплуатирующего персонала к техническим и программным средствам, а также информационным ресурсам АСЗИ.

Пользователям предоставляется право работать только с теми средствами и ресурсами, которые необходимы им для выполнения установленных функциональных обязанностей.

Полномочия разработчиков, пользователей и эксплуатирующего персонала по доступу к ресурсам АСЗИ устанавливаются заказчиком системы и отражаются в ТЗ на создание (модернизацию) АСЗИ в разделе "Положения о разрешительной системе допуска исполнителей к документам и сведениям на предприятии" и в инструкции по эксплуатации АСЗИ.

4.8 В АСЗИ защите подлежат:

- информационные ресурсы в виде информационных массивов и баз данных, содержащих защищаемую информацию, и представленные на магнитных, оптических и других носителях;
- средства автоматизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных и другие средства.

4.9 Система защиты информации в АСЗИ является неотъемлемой составной частью создаваемой АСЗИ или реализуется в виде дополнительной подсистемы модернизируемой функционирующей автоматизированной системы. Требования к системе защиты информации АСЗИ предъявляют согласно существующим нормативным документам.

5 Общие требования

5.1 Общие требования к АСЗИ включают:
- функциональные требования;
- требования к эффективности;
- технические требования;
- экономические требования;
- требования к документации.

5.2 Функциональные требования к АСЗИ включают следующие группы требований:
- грифы секретности (конфиденциальности) обрабатываемой в АСЗИ информации;
- класса защищенности АСЗИ;
- цели защиты информации;
- задачи защиты информации в АСЗИ;

- перечень защищаемой в АСЗИ информации и требуемые уровни эффективности ее защиты;

- возможные технические каналы утечки информации и способы несанкционированного доступа к информации, несанкционированных и непреднамеренных воздействий на информацию в АСЗИ, класс защищенности АСЗИ.

5.2.1 Определение грифа секретности (конфиденциальности) информации, категории защиты АСЗИ осуществляет заказчик в соответствии с действующими руководящими и нормативными документами в области защиты информации.

5.2.2 Определение класса защищенности АСЗИ осуществляется в соответствии с действующими нормативными документами.

5.2.3 Цели защиты информации в АСЗИ

5.2.3.1 Общей целью ЗИ в АСЗИ является предотвращение или снижение величины ущерба, наносимого владельцу и/или пользователю этой системы, вследствие реализации угроз безопасности информации.

Частными целями защиты информации, обеспечивающими достижение общей цели АСЗИ, являются:

- предотвращение утечки информации по техническим каналам;

- предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации;

- соблюдение правового режима использования массивов, программ обработки информации, обеспечения полноты, целостности, достоверности информации в системах обработки;

- сохранение возможности управления процессом обработки и использования информации условиях несанкционированных воздействий на защищаемую информацию.

5.2.3.2 Цели защиты информации в АСЗИ должны включать:

- содержательную формулировку цели защиты;

- показатель эффективности достижения цели и требуемое его значение;

- время актуальности каждой цели защиты информации (этапы жизненного цикла, в течение которых цель должна достигаться).

5.2.4 Формулировка каждой задачи защиты информации в АСЗИ должна включать:

- наименование конкретной угрозы безопасности для АСЗИ (ее компонента), которую необходимо предотвратить (устранить) при решении задачи;

- формулировку способа решения задачи;

- перечень функций, которые должны быть реализованы для решения данной задачи:

- требования к эффективности или гарантиям решения задачи;

- ограничения на ресурсы АСЗИ, выделяемые на решение данной задачи.

5.2.4.1 Задачи защиты информации в АСЗИ включают:

- предотвращение перехвата защищаемой информации, передаваемой по каналам связи;

- предотвращение утечки обрабатываемой защищаемой информации за счет побочных электромагнитных излучений и наводок;

- исключение несанкционированного доступа к обрабатываемой или хранящейся в АСЗИ защищаемой информации;

- предотвращение несанкционированных и непреднамеренных воздействий, вызывающих разрушение, уничтожение, искажение защищаемой информации или сбои в работе средств АСЗИ;

- выявление возможно внедренных в технические средства АСЗИ специальных электронных устройств перехвата информации;

- организация разрешительной системы допуска пользователей АСЗИ к работе с защищаемой информацией и ее носителями;

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

5.2.5 Перечень защищаемой информации в АСЗИ и требуемые нормы (уровни) эффективности ее защиты

5.2.5.1 Определение конкретного перечня защищаемой информации в АСЗИ должно осуществляться исходя из назначения АСЗИ, целей защиты информации, состава и структуры АСЗИ, а также состава и структуры защиты информации.

Перечень защищаемой информации определяется как для АСЗИ в целом, так и для ее составных частей (компонентов).

5.2.5.2 Требования по эффективности защиты информации в АСЗИ должны включать:

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

5.2.6 Выявление возможных технических каналов утечки информации в АСЗИ, способов несанкционированного доступа, несанкционированных и непреднамеренных воздействий на нее должно осуществляться на основе анализа состава, структуры, алгоритмов функционирования АСЗИ, условий размещения АСЗИ с использованием моделей угроз безопасности информации, номенклатуры воздействующих на информацию факторов в соответствии с действующими нормативными документами.

Оценка опасности технических каналов утечки информации, возможных способов несанкционированного доступа к информации и несанкционированных воздействий на нее осуществляется по показателям и методикам, определенным в нормативных и методических документах уполномоченного государственного органа на проведение соответствующих работ.

5.3 Требования к эффективности или гарантиям решения задач защиты информации в АСЗИ включают:

- требования по предотвращению утечки защищаемой информации по техническим каналам;
- требования по предотвращению несанкционированного доступа к защищаемой информации;
- требования по предотвращению несанкционированных и непреднамеренных воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств АСЗИ;
- требования по выявлению внедренных в помещения и в технические средства специальных электронных устройств перехвата информации;
- требования по контролю функционирования системы защиты информации АСЗИ.

5.3.1 Требования по предотвращению утечки защищаемой информации по техническим каналам.

5.3.1.1 Требования по предотвращению утечки защищаемой информации включают:

- требования по предотвращению утечки защищаемой информации за счет побочных электромагнитных излучений и наводок;
- требования по предотвращению утечки защищаемой информации по техническим каналам разведки;
- требования по предотвращению утечки защищаемой информации за счет сигналов, излучаемых техническими средствами АС, которые обеспечивают функционирование системы;
- требования по предотвращению утечки защищаемой информации за счет несанкционированного доступа к ней.

5.3.1.2 Средства вычислительной техники, входящие в состав АСЗИ и подлежащие защите, должны удовлетворять требованиям по защите информации от утечки за счет побочных электромагнитных излучений и наводок. Номенклатура показателей эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок определяется в соответствии с действующими нормативными документами.

5.3.1.3 Требования по предотвращению утечки защищаемой информации по техническим каналам разведки включают:

- требования по предотвращению утечки защищаемой информации по каналам технической разведки;
- требования по предотвращению утечки защищаемой информации по каналам агентурной разведки, использующей технические средства.

Требования по предотвращению утечки защищаемой информации по каналам технической и агентурной разведки устанавливают в соответствии с требованиями действующих нормативных документов.

5.3.1.4 Требования по устойчивости функционирования структурных компонентов АСЗИ к внешним факторам, воздействующим на информацию, устанавливают на конкретные классы (виды, типы) компонентов АСЗИ по ГОСТ 16325, ГОСТ 20397, ГОСТ 21552, ГОСТ 27201.

Требования по устойчивости АСЗИ к внутренним воздействующим факторам на информацию (отказы, сбои, ошибки) устанавливают совместно с требованиями надежности и устойчивости функционирования конкретной системы или ее компонентов и по ГОСТ 20397, ГОСТ 16325, ГОСТ 21552, ГОСТ 27201.

5.3.1.5 Требования по предотвращению утечки защищаемой информации за счет встроенных электронных и/или программных закладок в АСЗИ включают требования по выявлению встроенных закладочных устройств и их устранению. Эти требования устанавливают в соответствии с действующими руководящими и нормативными документами.

5.3.2 Требования по предотвращению несанкционированного доступа к защищаемой информации устанавливают по СТ РК ГОСТ Р 50739 и нормативным документам уполномоченного государственного органа.

5.3.3 Требования по предотвращению несанкционированных и непреднамеренных воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств АСЗИ информации, устанавливают в соответствии с действующими правовыми, руководящими и нормативными документами в области защиты информации.

Требования по предотвращению изменения информации за счет внешних воздействующих факторов на АСЗИ устанавливают с учетом требований, предъявляемых к компонентам АСЗИ по ГОСТ 20397, ГОСТ 21552, ГОСТ 27201.

Требования по предотвращению изменения защищаемой информации за счет внешних побочных явлений (электромагнитных полей) устанавливают в соответствии с нормами по электромагнитной совместимости и действующими нормативными документами.

Требования по предотвращению изменения защищаемой информации за счет субъективных преднамеренных действий злоумышленника на АСЗИ, включающих компьютерные вирусы, устанавливаются в соответствии с действующими нормативными документами и достигаются применением специальных программных и аппаратных средств защиты (антивирусные программы) и организации системы контроля безопасности программного обеспечения.

5.4 Технические требования по защите информации включают требования к основным видам обеспечения АСЗИ:

- техническому и программному;

- к зданиям (помещениям) или объектам, в которых АСЗИ устанавливаются, а также к средствам защиты информации и контроля эффективности защиты информации.

5.4.1 Требования по защите информации к техническому обеспечению АСЗИ включают требования как к основным техническим средствам, используемым по функциональному назначению АСЗИ, так и к вспомогательным техническим средствам, обеспечивающим функционирование основных технических средств.

5.4.1.1 Технические требования, предъявляемые к основным техническим средствам, содержат требования по защите информации от утечки по ПЭМИН, от закладных устройств, от внешних и внутренних воздействующих факторов, от несанкционированного доступа к информации и несанкционированных действий на нее.

5.4.1.2 Конструктивные требования, предъявляемые к техническим средствам АС, должны формироваться с учетом требований по защите информации и включаться в раздел "Конструктивные требования" ТЗ на разработку конкретного технического средства АСЗИ.

5.4.1.3 Технические средства АСЗИ должны обеспечивать сохранность информации при отключении электропитания, при авариях, а также в условиях неблагоприятных природных явления и стихийных бедствий.

5.4.1.4 Методы контроля, испытаний и приемки технических средств АСЗИ должны соответствовать ГОСТ 23773.

5.4.1.5 Требования к системе заземления и сети электропитания АСЗИ должны устанавливаться в соответствии с требованиями соответствующих нормативных документов.

5.4.2 Требования к защите сети телекоммуникаций (сети передачи данных) устанавливают в соответствии с требованиями соответствующих нормативных документов.

5.4.3 Требования по защите информации к программному обеспечению АСЗИ регламентируются действующими руководящими и нормативными документами в области защиты информации.

5.4.4 Требования по ЗИ к зданиям (помещениям) или к устройствам, в которых устанавливаются АСЗИ, включают требования к ограждающим конструкциям здания (помещения), к технологии строительства, требования к средствам коммуникаций и требования к звукоизоляции помещений.

5.4.4.1 При необходимости реконструкции и расширения помещений и сооружений объекта, на котором размещается АСЗИ, требования по защите информации предъявляют в соответствии со СНиП и другими действующими руководящими и нормативными документами.

5.4.4.2 При размещении основных технических средств АСЗИ в помещениях, предназначенных для ведения секретных (конфиденциальных) переговоров, должны быть приняты меры по защите от утечки речевой информации за счет акустоэлектрических преобразований в элементах основных и вспомогательных технических средств АСЗИ.

5.4.5 Требования, предъявляемые к средствам защиты информации и средствам контроля эффективности защиты информации

5.4.5.1 Номенклатуру и содержание требований, предъявляемых к средствам защиты информации и контроля эффективности защиты информации, определяют в соответствии с действующими нормативными документами и техническими условиями на средства защиты информации и контроля ее эффективности.

5.4.6 Ограничения на аппаратные, программные, информационные, временные и другие ресурсы АСЗИ, выделяемые на решение задач защиты информации, определяют с учетом имеющихся ресурсов АСЗИ исходя из допустимого снижения эффективности,

функционирования АСЗИ по основному функциональному назначению.

5.5 Экономические требования по ЗИ включают:

- допустимые затраты для организаций, заказывающих создание АСЗИ и/или системы защиты информации в АСЗИ;

- допустимые затраты для организаций, эксплуатирующих АСЗИ и/или системы защиты информации в АСЗИ.

5.6 Требования к документации на АСЗИ

5.6.1 Комплектность документации на АСЗИ устанавливается в нормативных документах и по ГОСТ 34.201 и дополнительно включает документы, указанные в таблице 1.

5.6.2 Требования к комплектности конструкторской, технологической и эксплуатационной документации на средства защиты информации и контроля ее эффективности

На технические средства разрабатывают конструкторскую и эксплуатационную документацию согласно требованиям ЕСКД.

Таблица 1 - Номенклатура дополнительной документации по защите информации на автоматизированную систему

Наименование документа	Код документа по ГОСТ 34.201	Примечание
1 Схема первичного электропитания основных и вспомогательных технических средств АСЗИ	С7*	С учетом требований по ЗИ
2 Схема заземления основных и вспомогательных технических средств АСЗИ	С7*	С учетом требований по ЗИ
3 Спецификация основных и вспомогательных технических средств, программных средств АСЗИ	-	
4 Руководство для абонентов АСЗИ (сети) по режимным вопросам	ИЭ4	С учетом требований по ЗИ
5 Перечень контрольных испытаний и проверок (объем и периодичность) по подтверждению защищенности АСЗИ	-	
6 Предписание на эксплуатацию ТС	Д130	С учетом требований по ЗИ
7 Сертификат соответствия (на каждое ТС, ПС системы и СрЗИ)	-	
8 Акт категорирования средств АСЗИ и системы в целом по вопросам защиты информации	-	
9 Акт классификации АСЗИ в части защиты от НСД к информации в системе	-	
10 Документ, подтверждающий соответствие АСЗИ требованиям НД по защите информации	-	

Наименование документа	Код документа по ГОСТ 34.201	Примечание
11 Формуляр по защите информации (технический паспорт)	-	
12 Концепции, положения, руководства, наставления, инструкции, уставы, правила, нормы, модели.	-	
* Документы, код которых установлен в соответствии с требованиями стандартов ЕСКД		

Окончание таблицы 1

На программные средства разрабатывают конструкторскую и эксплуатационную документацию в соответствии с ЕСПД.

На программно-технические средства разрабатывают конструкторскую и эксплуатационную документацию согласно требованиям ЕСПД, ЕСКД и ЕСТД.

5.6.3 Требования к составу, видам документов и содержанию организационно-распорядительной документации устанавливают в соответствии с действующими руководящими и нормативными документами.

Приложение
(справочное)

Библиография

[1] Закон Республики Казахстан «О государственных секретах»

[2] Концепция информационной безопасности Республики Казахстан, утвержденная Указом Президента РК от 10.10.2006 № 199

Для заметок

УДК 681.3 **МКС 35.040**

Ключевые слова: защищаемая информация, автоматизированная система, автоматизированная система в защищенном исполнении, требования по защите информации, средства защиты информации, средства контроля эффективности защиты информации, система защиты информации, сертификация средств защиты информации, контроль эффективности защиты информации

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