ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

МЕМЛЕКЕТТІК СТАНДАРТТАР ҚОРЫНЫҢ АҚПАРАТТЫҚ ЖҮЙЕСІН РҰҚСАТ ЕТІЛМЕГЕН АҒЫМДАРДАН ҚОРҒАУ

Жалпы техникалық талаптар

ҚР СТ 1178-2003

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігінің Стандарттау, метрология және сертификаттау жөніндегі комитеті (Мемстандарт)

Астана

Алғы сөз

1 “Қазақстан Стандарттау және сертификаттау институты” **РМК ӘЗІРЛЕП ЕНГІЗГЕН**

2 Қазақстан Республикасы Индустрия және сауда министрлігінің Стандарттау Метрология және сертификаттау жөніндегі комитетінің 2003 жылғы 07 қарашадағы № 382 бұйрығымен **БЕКІТІЛІП ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ **2009 жыл**
ТЕКСЕРУ КЕЗЕҢДІЛІГІ **5 жыл**

4 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТҚК СТАНДАРТЫ

МЕМЛЕКЕТТІК СТАНДАРТТАР ҚОРЫНЫҢ АҚПАРАТТЫҚ ЖҮЙЕСІН РҰҚСАТ ЕТІЛМЕГЕН АҒЫМДАРДАН ҚОРҒАУ

Жалпы техникалық талаптар

Енгізілген күні 2004-09-01

1 Қолданылу саласы

Осы стандарт Мемлекеттік стандарттар қорының Ақпараттық жүйесін (МСҚ АЖ), сондай-ақ стандарттау, метрология және сертификаттау жөніндегі Дүниежүзілік сауда ұйымымен (ДСμ) бірігіп әрекет ететін Ақпараттар жүйесін рұқсат етілмеген ағымдардан (РЕА) қорғау үшін есептеуіш техника құралдарына (ЕТҚ) қойылатын біріңғай функционалды талаптарды бекітеді. Ақпаратты РЕА-дан қорғау дәрежесі бойынша ЕТҚ сипаттамасын анықтайтын және қорғауға қойылатын талаптардың жиынын анықтайтын ЕТҚ-ның қорғау көрсеткіштерінің номенклатурасына қойылатын талаптарды бекітеді.

ЕТҚ комплектінде ақпаратты криптограммалық қорғау құралдары қорғаудың сапасын көтеру үшін пайдалануы мүмкін.

Осы стандарттың талаптары стандарттау, метрология және сертификаттау жөніндегі уәкілетті органдарға, оларға қарасты Қазақстан республикасының Мемлекеттік стандарттар қорының құрамына кіретін мемлекеттік кәсіпорындар мен құрылымдық кәсіпорындарға міндетті болып табылады.

2 Нормативтік сілтемелер

Осы стандартта келесі нормативтік құжаттарға сілтемелер қолданылған:

ҚР СТ 34.013-2002 Ақпараттық технология. Есептеу техникасы құралдарында ақпараттар әзірлеу барысында түзетулер енгізу кезінде және электромагнитті сәулелер ағымы бойынша ақпараттарды қорғау. Жалпы техникалық талаптар.

ҚР СТ ИСО 9000-2001 Сапа менеджменті жүйесі. Жалпы талаптар.

ГОСТ 7.0 СИБИД. Ақпараттық-кітапханалық қызмет, библиография. Терминдер мен анықтамалар.

ГОСТ 19.105-78 Бағдарламалық құжаттамалардың бірыңғай жүйесі. Бағдарламалық құжаттамаларға қойылатын жалпы талаптар.

Ресми басылым

3 Анықтамалар

Осы стандартта келесі терминдер мен оларға сәйкес анықтамалар қолданылады:

3.1 Есептеу техникасы құралдары: Мәліметтерді әзірлеу барысында өздігінен сараптама жасай алатын немесе өзге де жүйелерді қамти алатын бағдарламалық және техникалық элементтер жүйесі.

3.2 Техникалық қорғау құралдары: техникалық, аппараттық (механикалық, оптикалық, радио-, радиолокалдық, электрондық) құралдар немесе өздігінен және кешенді түрде өзге құралдармен бірігіп ақпаратты қорғау қызметін атқаратын жүйе (ҚР СТ 34.013).

3.3 Ақпараттық ресурстар: Растылық ақпараттарды тиімді түрде алу үшін ұйымдастырылған мәліметтер жиынтығы (ГОСТ 7.0).

3.4 Ақпараттық технология: Ақпаратты тарату және алмастыру, көшірмесін алу, шығару, іздеу қайта өңдеу, жинау, сақтау, жасау, жинақтау жұмыстарын қамтамасыз ететін, технологиялық комплектіге біріктірілген бағдарламалық-техникалық құралдар мен өндірістік үрдістер, әдістемелер жиынтығы (ГОСТ 7.0).

3.5 Ақпараттық сеть: коммуникация жүйесі және электронды техника саласына жататын біріңғай техникалық құралдар жиынтығы.

3.6 Мәліметтер базасы: мынадай қасиеттері бар мәліметтер жиынтығы: өзара байланысты; жалпы тапсырмаларға интеграциялық және жобалау қабілеттілігі; шындық өмірге тән моделділік; қолданбалы бағдарламаларда мәліметтерді сипаттаудағы тәуелсіздік.

3.7 Верификация: қойылған талаптардың орындалғаны жөнінде объективті куәлерді көрсету арқылы бекіту (ҚР СТ ИСО 9000-2001).

4 Жалпы талаптар

4.1 Мемлекеттік стандарттар қорының Ақпараттық жүйесі стандарттау, метрология және сертификаттау туралы нормативті құжаттар бойынша ақпараттарды сақтау, әзірлеу, іздеу, тарату, беру және ұсыну жұмыстарына бағытталған.

ДСҰ-мен бірігіп әрекет ету жөніндегі ақпараттар жүйесі ДСҰ Секретариатымен, халықаралық ұйымдармен бірігіп әрекет етуге, стандарттар мен сәйкестігін бағалау үрдісіне қатысты ақпараттар мен құжаттамаларға сәйкес қызығушылығы бар тұлғаларды таныстыруға да арналған.

4.2 МСҚ АЖ қорғау талаптары бағдарламалық-техникалық қорғау құралдарының жиынтығы түрінде таратылады. ГОСТ 19.105 сәйкес бағдарламалық құжаттарды” жалпы талаптары.

Барлық қорғау құралдарының жиынтығы қорғау құралдарының кешенін (ҚҚК) құрайды.

4.3 МСҚ АЖ қорғау көрсеткіштері ЕТҚ қорғау класына қатысты дәрежесі мен тереңділігі бойынша варьиерленген талаптары арқылы сипаталады, осы стандартта кез келген көрсеткішке ЕТҚ қорғауда ең жоғарғы класқа сай келетін талаптар тобы қойылады.

4.4 МСҚ АЖ қолданыстағы ақпараттарды қауіпсіздік талаптары деңгейіне сәйкес қорғауды қамтамасыз етуі тиіс, соның ішінде:

- ішкі бағыттармен берілетін ақпараттар сертификатталған ақпараттық немесе бағдарламалық криптограммалық құралдардың көмегімен қорғалуы тиіс;

- МСҚ АЖ пайдалануда қолданушының тұтыну құқығы шектеулі болуын қамтамасыз етуі тиіс;

Интернеттің телекоммуникациялық желісі арқылы енген бөгде адамдардың рұқсат етілмеген бағыттары жойылуы тиіс.

4.5 Ақпараттық ресурстардың қауіпсіздігі мәліметтер базасын (МБ) басқару жүйесінде қолданылатын дайын құралдармен, қорғалатын ақпараттарға түсетін жолдарды бақылайтын оригинал бағдарламалар жабдығымен қамтамасыз етілуі тиіс.

5 Мемлекеттік стандарттау қорының ақпараттық жүйесін қорғау құралдарының сипаттамасы

5.1 Ақпаратты техникалық қорғау құралдарының түрлері.

5.1.1 Осы стандарт ақпаратты техникалық қорғау құралдарының мынадай түрлерін бекітеді:

- ақпараттарды рұқсат етілмеген ағымдардан (РЕА) қорғау жабдықтары;

- ақпараттарды қорғау құралдарына арналған бағдарламалық қамсыздандыру;

- ақпараттарды өңдеуге арналған қорғанышы бар бағдарламалық жабдықтар;

- ақпараттарды қорғаудың бағдарламалық-техникалық жабдықтары.

5.2 Ақпараттарды РЕА-дан техникалық қорғау құралдарының сипаттамасы

5.2.1 Ақпараттарды РЕА-дан техникалық қорғау құралдарына мыналар жатады:

- белсенді емес қорғау құралдары, соның ішінде:

а) құлыптар (микропроцессормен басқарылатын, радиобасқару және т.б.);

б) әр түрлі электрлі датчиктер;

в) күзет және бақылаудың телевизиалық жүйесі;

з) желілер жүйесі;

к) сәйкестік құралдары, шектеулер;

л) ережені бұзушыны немесе бұзу әрекеттерін қолға түсіру құралдары;

м) ақпараттарды физикалық тасымалдайтын құралдарды (стримерлер таспасы, магниттік және оптикалық дискілер және т.б.) сақтауға және тасымалдауға арналған арнайы құралдар.

5.3 Ақпаратты қорғаудың бағдарламалық-техникалық құралдарының сипаттамасы

Ақпаратты бағдарламалық-техникалық қорғау құралдарына мыналар жатады:

- ақпарат алуда ережені бұзу барысында қолданушының бағдарламасын үзу құралы;
- мәліметтерді өшіру құралы;
- РЕА жасау барысында дабыл қағу құралы;
- электрондық салымдарды оқшаулау құралы;
- ақпараттық технологиялардағы дайын ақпараттарды алуға шектеу қоятын бағдарламалы-аппараттық құралдар.

5.4 Ақпаратты қорғау құралдарының бағдарламалық сипаттамалары.

Ақпаратты қорғау құралдарының бағдарламаларына мыналар жатады:

- мандат, дискретті немесе көп деңгейлі түйсіктер (матрица және ағымдар диспетчері, ақпараттарға түсіретін қолданушының электронды журналы, құпия белгілер және т.б.) бойынша ақпараттар ағыма қойылатын шектеулерді қамтамасыз ететін бағдарламалар;
- әр түрлі белгілеулер (кілт сөз, қосымша код сөзі, биомериялық мәліметтер және т.б.) бойынша қолданушылар мен терминалдардың идентификациялау және аутентификациялау бағдарламалары, соның ішінде идентификациялаудң (аутентификациялаудың) жоғарылау бағдарламалары;
- РЕА-дан ақпаратты қорғау жүйесінің қызмет етуін қадағалау бағдарламалары;
- қорғау құралдарының бүтіндігін тексеру бағдарламалары;
- көмекші негізіндегі әр түрлі қорғау бағдарламалары, соның ішінде вирусқа қарсы бағдарламалар;
- қолданбалы электронды-эсептеуіш машиналарының операциялық жүйелерін қорғау бағдарламалары (модулді бағдарламалық интерпретация және т.б.);
- жалпыжүйелік және қолданбалы бағдарламамен қамсыздандырудың бүтінділігін бақылау бағдарламалары;
- ресурстарды пайдалану барысында ереженің бұзылғаны туралы дабыл қағатын бағдарламалар;
- сыртқы есте сақтау құрылғыларының файлдық құрылымдарына және қалпына келтіру құралдарын бақылау бағдарламалары;
- жүйе жұмысының емістеуі немесе РЕА фактілері ұсталған жағдайда оны блоктау бағдарламалары;

- РЕА фактілерін ұстау және оларды ұстаған жағдайда дабыл қағу (хабар жіберу) бағдарламалары;
- бағдарламалық салымдарды оқшаулау және ұстау бағдарламалары;
- өлшеу нәтижелерін өңдеу бағдарламалары және тестілеу бағдарламалары;
- Интернеттегі РЕА қорғау үшін бағдарламалық қамсыздандыру.

6 Жалпы техникалық талаптар

6.1 Ақпаратты ЕТҚ өңдеу барысында РЕА-дан қорғау уәкілетті тұлға немесе олармен талап етілген үрдістер арқылы ғана ақпаратты оқуға, жазуға, жасауға және жоюға жол ашуымен сипатталады.

Қорғау ЕТҚ әрекет ететін қорғау құралдарына қойылған үш түрлі талаптармен қамтамасыз етіледі:

а) ЕТҚ түсетін ағымдарды шектеу туралы белгілі бір ережелердің қайшылықтар тудырмауы туралы қарастырылған ағымдарға шектеу қою талаптары;

б) ақпаратты қорғауға қатысы бар жағдайлар ЕТҚ-да тіркелгені туралы қарастырылған есептерге қойылатын талаптар;

в) ЕТҚ түрлі ағымдар мен есептерге қойылатын талаптардың орындалуын қамтамасыз ететіні жөнінде кепілдік бере алатын ЕТҚ құрамындағы техникалық және бағдарламалық механизмдер болған жағдайда берілетін кепілдемеге қойылатын талаптар;

6.2 Ағымдарға шектеу қою талаптары

6.2.1 Ағымдарға шектеу қою талаптары ЕТҚ болуы тиіс мынадай қорғау көрсеткіштерін анықтайды:

а) ағымды бақылаудағы дискретизациялық принцип;

б) ағымды бақылаудағы мандаттық принцип;

в) идентификация мен аутентификация;

г) жадыны тазалау;

д) модулдерді оқшаулау;

е) ақпаратты тасымалдайтын аласталған физикалық тасымал құралына жазуды және алуды қорғау;

ж) қолданушының құралдарға бағынуы.

6.2.2 Ағымды бақылаудың дискретизациялық принциптерін жүзеге асыру үшін қорғау құралдарының кешені (ҚҚК) атаулы субъектілердің (қолданушылардың) атаулы объектілерге (мысалы, файлдарға, бағдарламаларға, мәліметтер базасына) түсетін ағымдарына бақылау жүргізуі керек.

Әр жұпқа (субъект-объект) ЕТҚ мүмкін болатын ағымдар түрлері (мысалы, оқу, жазу) анық және екі ұшты ойсыз бөлініп берілуі тиіс, соның

ішінде сол жекелік субъектілерге немесе жекелеген топтарға (ЕТҚ обкъектісі берілген ресурстарда) рұқсат етілген ағымдар түрлеріне.

Ағымды бақылау әр объектіге, әр субъектіге (жеке және бір құқықты жекеліктерге) қолданылуы тиіс.

Ағымды бақылаудың дискретизациялық принциптерін жүзеге асыратын механизм ағымдарды шектейтін ережелерге (АШЕ) рұқсат етілген өзгертулерді қарастыруы қажет, соның ішінде қорғалатын объект тізімін және ЕТҚ қолданушылар тізіміндегі рұқсат етілген өзгертулерді қарастыруы қажет.

Ағымдарды шектеу ережелерін өзгерту құқығы бөлінген объектіге (мысалы, әкімшілік, қауіпсіздік қызметі) берілуі қажет.

Ағымға түсу құқығын таратуды шектейтін басқару жабдығы қарастырылуы қажет.

Қорғау құралдарының кешені айқын әрекеттегі қолданушы сияқты жасырын әрекетегі қолданушының да ағымдарды шектеу ережесі (АШЕ) дискретизациялық өмірінде қайталанатын механизмді қарастыруы керек. Бұл жерде “айқын” деп жүйелік құрылғыларды қолдана отырып жасалған әрекеттерді, “жасырын” деп өзге әрекеттер, сондай-ақ өзіндік бағдарламаларды қолданып, құрылғылармен жұмыс істеген әрекеттерді айтамыз.

6.2.3 Ағымды бақылаудың мандатты принциптерін жүзеге асыру үшін әр субъектіге және әр объектіге иерархиясына сәйкес орындарында айқындалатындай белгілеулеріне сипаттама беріліп, бекітілуі қажет. Осы белгілеулердің көмегімен субъектілер мен объектілерге иерархиялық сипаттамалар мен иерархиялық санаттарының дәрежесінің қиысуы болып табылатын сипаттамалық дәрежесі бекітілуі қажет. Берілген белгілеулер ағымды шектеудің мандатты принциптерінің негізі болып қызмет атқаруы қажет.

Қорғау құралдарын бақылауда жүйеге жаңа мәліметтерді енгізу барысында рұқсат етілген қолданушыдан осы мәліметтерді” сипаттамалық белгілеулерін сұрап алуы қажет. Қолданушылар тізіміне жаңа субъектіні қосу үшін рұқсат етілген өзгертулер енгізуге оның сипаттамалық белгілеулері бекітілуі қажет. Субъектінің (объектінің) сыртқы сипаттамалық белгілеулері олардың ішкі сипаттамалық белгілеулерімен (ішкі ҚҚК) дәлме-дәл сәйкес келуі қажет.

Құралдарды қорғау кешені (ҚҚК) ағымдарды бақылаудың мандатты принциптерін кез-келген субъект тарапынан келетін айқын және жасырын объектілер ағымына қолданылып, жүзеге асырылуы қажет:

а) субъект объекті оқи алады, егер объектінің сипаттамалық деңгейіндегі иерархиялық сипаттамасы субъектінің сипаттамалық деңгейіндегі иерархиялық сипаттамасы деңгейінен аз болмаса және субъектінің сипаттамалық деңгейіндегі иерархиялық санаттарында объектінің

сипаттамалық деңгейіндегі барлық иерархиялық емес санаттары қосылып көрсетілсе;

б) субъект объектіге көшіріп жаза алады, егер субъектінің иерархиялық сипаттамасындағы сипаттамалық деңгейі объектінің иерархиялық сипаттамасындағы сипаттамалық деңгейінен аз болмаса және субъектінің сипаттамалық деңгейіндегі барлық иерархиялық емес санаттарында объектінің сипаттамалық деңгейіндегі иерархиялық емес санаттары қосылып көрсетілсе.

Мандатты АШЕ (ағымдарды шектеу ережесі) субъектілер мен арнайы бөлінген субъектілері бар объектілердің сипаттамалық деңгейін өзгерту жолдарының мүмкіндіктерін қарастыруы қажет.

ЕТҚ ағымдар диспечері қызмет етуі қажет, соның ішінде барлық субъектілердің объектілерге шығуын ұстауды жүзеге асыратын құрал, сондай-ақ ағымдарды шектеуге тапсырылған принциптерге сәйкес ағымдарды шектеу диспечері қызмет етуі қажет. Бұл орайда ағымға түскен рұқсат етілмеген сұраныс туралы шешімді оның дискредитациялық және мандаттық ағымдарды шектеу ережелерінің қатар рұқсат беруі барысында ғана қабылдау қажет болады. Осылайшы, тек ағымның біріңғай актін ғана емес, ақпараттар ағымын да бақылап отыру қажет болады.

6.2.4. ҚҚБ ағымға сұраныс барысындағы субъектілердің жекелігін қамтамасыз етуі қажет, субъектінің жекелігінің шынайы екендігін тексеріп, аутентификацияны жүзеге асыруы қажет. ҚҚБ идентификация мен аутентификация үшін керекті мәліметтерге ие болуы қажет және аутентификация барысында шынайылығы анықталмаған субъектілер немесе идентификацияланбаған субъектілердің қорғаудағы ресурстарына түсетін ағымдарға кедергі жасауы қажет.

ҚҚБ-да берілген субъектіге қатысты қолданылған бақылауларға қатысы бар барлық әрекеттердің алынған идентификациялық және аутентификациялық нәтижелерін байланыстыра білу қабілеті болуы қажет.

6.2.5 ҚҚБ оперативті және сыртқы жадыны тазалауды жүзеге асыруы қажет. Тазалау жадының босауы (қайта реттелуі) барысында перделенген ақпаратты жазу арқылы жүзеге асады.

6.2.6 ЕТҚ мультибағдарламалардың ұсталуы барысында ҚҚК басқа процессордың бағдарламалық модулінен келесі бір процессордың бағдарламалық модуліне изоляция жасайтын бағдарламалы-техникалық механизмді жүзеге асыруы қажет, сондай-ақ әр түрлі қолданушылардың ЭЕМ оперативті жадындағы бағдарламалар бір-бірінен қорғалуы қажет.

6.2.7 ҚҚК әрбір енгізу-шығару құрылғысын және әрбір арнайы пайдаланылатын немесе идентификациялы (белгіленген) байланыс арналарын ажырата білуі қажет. Белгіленген құрылғыдан шығару (белгіленген құрылғыға енгізу) барысында ҚҚК енгізілетін (шығарылатын) объекті (сипаттамалық деңгейде) белгілеулері мен құрылғының белгілеулері

арасындағы сәйкестікті қамтамасыз етуі керек. Осындай сәйкестік “белгіленген” байланыс арнасының жұмыс барысында да болуы қажет.

Құрылғылар мен арналарды таңбалау және орнықтыруларын өзгерту ісі тек ҚҚК бақылауымен ғана жүзеге асырылуы қажет.

6.2.8 ҚҚК қолданушының сұранымындағы құрылғыларды арнайы қолданатын қрылғылар сияқты идентификациялы құрылғыларда да (маркі таңбалары сәйкес келген жағдайда) ақпараттарды берумен қамтамасыз етуі қажет.

ҚҚК-де рұқсат етілген қолданушыға бөлінген идентификациялы құрылғының көмегімен сенімді түрде қолдана алу механизмі болуы қажет.

6.3 Есеп жүргізуге қойылатын талаптар

6.3.1 Есеп жүргізуге қойылатын талаптар ЕТҚ-да болуы тиіс мынадай қорғау көрсеткіштері арқылы анықталады:

- тіркеу;
- құжаттарды маркілеу.

6.3.2 ҚҚК мынадай жағдайларды тіркеуді жүзеге асырып отыруы қажет:

а) идентификациялық және аутентификациялық механизмдердің қолданылуы;

б) қорғалатын ресурстарға сұранымның пайда болуы (мысалы, файлдардың немесе бағдарламалардың ашылуы);

в) объектіні жасау және жою;

г) ағымдарды шектеу ережесінің өзгеруіне байланысты туындайтын әрекеттер. Осы жағдайлардың әрбіріне мынадай ақпараттар тіркеліп отырылуы қажет:

- күні және уақыты;
- тіркелген жағдайларды жүзеге асырушы субъект;
- жағдайлардың түрлері (егер ағымның сұранысы тіркелген болса, онда объект немесе ағым түріне белгі қойылады);
- жағдай сәтті аяқталуын немесе аяқталмауын (ағымның сұранысына қызмет көрсетілді ме, жоқ па).

ҚҚК-де тіркелген ақпараттармен іріктеп танысатын құрал болуы қажет.

ЕТҚ қорғаудың жоғарғы класы үшін операторлар мен бөлінген субъектілердің (мысалы, қорғау әкімшілігі) ағымға түсуге тырысқан барлық әрекеттерін тіркеп отыру мүмкіндігі қарастырылуы қажет.

6.3.3 ҚҚК қорғаудағы ақпараттарды құжаттап шығару кезінде оның сипаттамалық белгілерін де шығаруды қамтамасыз етуі қажет.

6.4 Тұрақтылықтан бас тарту талаптары

6.4.1. Тұрақтылықтан бас тарту талаптары ЕТҚ болуы тиіс қорғаудың мынадай көрсеткіштерімен анықталады:

а) көшіруді” резервті әдістемесі;

б) қайта қалпына келтірудің сенімділігі;

в) ҚҚК-нің бүтінділігі;

г) түрлендіруді бақылау;

д) дистрибутивтілікті бақылау;

е) ҚҚК-мен қолданушының өзара әрекеттері;

ж) тестілеу.

6.4.2 ҚҚК алғашқы жобалау кезеңінде ағымды шектеу принциптерін және ағымды басқару механизмін беріп отыратын қорғау моделі құрылуы қажет. Бұл моделде:

а) қайшы келмейтін АШП (ағымдарды шектеу принциптері);

б) АШП өзгертуге қайшы келмейтін ережелер;

в) енгізу-шығару қрылғыларымен жұмыс істеу ережелері;

г) ағымды басқару механизмінің формалді моделі.

ҚҚК-нің ағымды басқару механизмі және оның қосымшаларының ерекше бөлшектері жоғары дәрежелі болуы қажет. Бұл ерекшеліктер ағымды шектеу принциптеріндегі мәліметтерге сәйкес анықталуы тиіс.

6.4.3 Жабдықтардың жұмысынан жаңылуы және бас тартуынан кейінгі толық қайта қалпына келтіруді ҚҚК-нің толығымен қайта қалпына келтіру қабілеттілігі қамтамасыз етуі қажет.

6.4.4 ҚҚН-нің бағдарламалық және ақпараттық бөлігінің бүтіндігін қадағалап отыру үшін ЕТҚ-да қажетті қабілеттілік болуы қажет.

ҚҚК бағдарламалары оперативті жадының жеке бөліктерінде орындалуы қажет. Бұл қойылған талаптар верификацияға берілуі тиіс.

6.4.5 ҚҚК жобалау, құру және жүргізу барысында ЕТҚ-ның кескінін басқару, сондай-ақ формалді моделдердегі, ерекшеліктердегі (әр деңгейдегі), құжаттамалардағы, мәтіндердегі, объекті кодтары бар мәліметтердегі өзгертулерді басқару ісі қарастырылуы қажет. Бағдарламаның мәтіні мен құжаттамалар арасында сәйкестік болуы қажет. Генеризацияланған мәліметтер бір-бірімен салыстырылуы қажет. Оригинал бағдарламалар қорғауда болуы керек.

6.4.6 ЕТҚ-да оригиналдардың көшірмесін алу барысында ҚҚК көшірменің дәлдігі бойынша бақылау ісі жүзеге асуы қажет. Дайындалған көшірме үлгіні қайталай алатынына кепілдік бере алуы қажет.

6.4.7 ҚҚК-де барлық субъектілер мен объектілердің ағымға түсуін ұстайтын диспечерлік механизмі болуы қажет.

6.4.8 ҚҚК-де өзін оқып, сараптау, верификациялау және модификациялау істерін жүзеге асыратын айқын анықтай алатын және модульді құрылымы болуы қажет. Қолданушы және ҚҚК сенімді интерфейспен қамтамасыз етілуі қажет (мысалы, жүйеге ену, ҚҚК мен қолданушылар сұранысы). Қолданушылар мен ҚҚК-нің әрбір интерфейсі осы сияқты басқа да интерфейстерде логикалық негізде оқшау тұруы қажет.

6.4.9 ЕТҚ-да тестілеу қажет:

а) ағымды шектеу принциптерін жүзеге асыру (ағымға түскен айқын және жасырын сұраныстарды ұстау, ағымға түскен рұқсат етілмеген және

рұқсат етілмеген сұраныстарды дұрыс анықтау, ағымды шектеу механизмінің функционалды құралдары, АШП-ға және тағы басқаларға рұқсат етілген өзгерістер енгізу);

б) оперативті және сыртқы жадыны тазалау;

в) оперативті жадыдағы процестерді оқшаулау механизмінің жұмысы;

г) құжаттамаларды маркілеу;

д) аласталған физикалық тасымалдау құралына ақпаратты енгізу-шығаруды және қолданушының құрылғысына тасымалдауды қорғау;

е) идентификация мен аутентификация, сондай-ақ оны қорғау құралдары;

ж) жағдайлардың тіркеу, тіркелген ақпараттарды қорғау құралы және олармен танысудың рұқсат етілген мүмкіндіктері;

з) қайта қалпына келтірудің сенімді механизмінің жұмысы;

и) ҚҚК-нің бүтіндігін бақылауды жүзеге асыратын механизмнің жұмысы;

к) дистрибуцияны бақылауды жүзеге асыратын механизмнің жұмысы.

7 Құжаттамаларға қойылатын талаптар

7.1 ЕТҚ пайдалану барысында, олардың сертификатталуы және басқа да түрлерін сынау кезінде ҚҚК-нін жан-жақты және тиянақты сипаттау қажет, сондай-ақ мынадай жайттар бекітілген құжаттамалар қажет:

а) қолданушылар жетекшілігі;

б) ҚҚК бойынша жетекшілік

в) тестілік құжаттамалар;

г) конструкторлық (жобалық) құжаттамалар.

7.1.1 Қолданушылар жетекшілігінде ҚҚК-нін пайдалану жолдарының және оның қолданушымен байланыстылығы туралы қысқаша сипаттама болуы қажет.

7.1.2 ҚҚК бойынша жетекшілік әкімшілік қорғауға бағытталған және мынадай мазмұнда болуы қажет:

а) бақылаудағы функциялардың сипаттамалары;

б) ҚҚК генерациясы бойынша жетекшілік;

в) ЕТҚ-ның старт сипаттамасы және старттың дұрыстығын тексеретін үрдістің сипаттамасы;

г) тіркеу құралымен жұмыс істеу үрдісінің сипаттамасы;

д) қайта қалпына келтірудің сенімді құралдары бойынша жетекшілік;

е) модификация және дистрибуцияны бақылау құралдары бойынша жетекшілік.

7.1.3 Тестілік құжаттамаларда ЕТҚ-на салынған тестілеулер мен сынақтардың сипаттамасы, сондай-ақ тестілеу нәтижелері болуы қажет.

7.1.4 Конструкторлық (жобалық) құжаттамалар мынадай мазмұнда болуы керек:

а) ЕТҚ жұмысы принциптерінің жалпы сипаттамасы;

б) ҚҚК-нің жалпы сызбасы;

в) ҚҚК-нің сыртқы интерфейстерінің және ҚҚК модулінің интерфейстерінің сипаттамасы;

г) қорғау моделінің сипаттамасы;

д) ағымдар диспечерінің сипаттамасы;

е) ҚҚК бүтіндігін бақылайтын механизмнің сипаттамасы;

ж) жадыны тазалау механизмінің сипаттамасы;

з) оперативті жадыдағы бағдарламаларды оқшаулау механизмінің сипаттамасы;

и) аласталған физикалық тасымалдау құралына ақпаратты енгізу-шығаруды және қолданушының құрылғысына тасымалдауды қорғау құралының сипаттамасы;

к) идентификация және аутентификация механизмінің сипаттамасы;

л) тіркеу құралының сипаттамасы;

м) ҚҚБ және оның интерфейстерінің жоғары дәрежелі спецификасын сипаттамасы;

н) ҚҚК қорғау құралының жоғары дәрежелі спецификасына сәйкестік верификациясының сипаттамасы;

о) дискретизациялық және мандаттық ағымдарды шектеу принциптерінің (АШП) эквиваленттілігі және жобалау кепілдігінің сипаттамасы.

ӘОЖ 681.32:006354 **МСЖ 35.100**

Түйінді сөздер: есептеу техникасы құралдары, ақпаратты рұқсат етілмеген ағымдардан қорғау, қорғау құралдарының кешені, қорғау құралдарына қойылатын талаптар

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

ЗАЩИТА ИНФОРМАЦИИОННОЙ СИСТЕМЫ ГОСУДАРСТВЕННОГО ФОНДА СТАНДАРТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Общие технические требования

СТ РК 1178-2003

Издание официальное

Комитет по стандартизации, метрологии и сертификации Министерства индустрии и торговли Республики Казахстан (Госстандарт)

Астана

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН РГП «Казахстанский институт стандартизации и сертификации»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Комитета по стандартизации, метрологии и сертификации Министерства индустрии и торговли Республики Казахстан № 382 от 07 ноября 2003 года

Требования разделов 6, 7 настоящего стандарта гармонизированы с ГОСТ Р 50739-95 «СВТ. Защита от несанкционированного доступа к информации. ОТУ» в части группы требований и требований к документации

3 СРОК ПЕРВОЙ ПРОВЕРКИ **2009 год**
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ **5 лет**

4 ВВЕДЕН ВПЕРВЫЕ

Содержание

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

ЗАЩИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ ГОСУДАРСТВЕННОГО ФОНДА СТАНДАРТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. Общие технические требования

Дата введения

1 Область применения

Настоящий стандарт устанавливает единые функциональные требования к защите средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) к Информационной системе Государственного фонда стандартов (ИС ГФС), в том числе к информационной системе по взаимодействию со Всемирной Торговой Организацией (ВТО) по стандартизации, метрологии и сертификации. Устанавливает требования к номенклатуре показателей защищенности СВТ, описываемых совокупностью требований к защите и определяющих классификацию СВТ по уровню защищенности от НСД к информации.

Применение в комплекте СВТ средств криптографической защиты информации может быть использовано для повышения гарантий качества защиты.

Требования настоящего стандарта являются обязательными для уполномоченного органа по стандартизации, метрологии и сертификации, подведомственных ему государственных предприятий и структурных предприятий, входящих в состав Государственного фонда стандартов Республики Казахстан.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

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

СТ РК ИСО 9000-2001 Системы менеджмента качества. Основные положения

ГОСТ 7.0-99 СИБИД. Информационно-библиотечная деятельность, библиография. Термины и определения

ГОСТ 19.105-78 Единая система программной документации. Общие требования к программным документам

Издание официальное

3 Определения

В настоящем стандарте использованы следующие термины с соответствующими определениями:

3.1 Средства вычислительной техники: совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

3.2 Технические средства защиты: технические, аппаратурные (механические, оптические, радио-, радиолокационные, электронные) устройства или системы, способные самостоятельно или в комплексе с другими средствами выполнять функции защиты информации (СТ РК 34.013)

3.3 Информационные ресурсы: совокупность данных, организованных для эффективного получения достоверной информации (ГОСТ 7.0)

3.4 Информационная технология: совокупность методов, производственных процессов и программно-технических средств, объединенных в технологический комплекс, обеспечивающий сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, передачу и распространение информации (ГОСТ 7.0)

3.5 Информационная сеть: система коммуникации и совокупность однородных технических средств, расположенных в отрасли электронной техники

3.6 База данных: совокупность данных, обладающих следующими свойствами: взаимосвязанностью; интегрированностью и ориентацией на общие задачи; модельностью, отражающей часть реального мира; независимостью описания данных от прикладных программ

3.7 Верификация: подтверждение, посредством представления объективных свидетельств того, что установленные требования были выполнены (СТ РК ИСО 9000-2001)

4 Общие требования

4.1 Информационная система Государственного фонда стандартов предназначена для хранения, обработки, поиска, распространения, передачи и предоставления информации по нормативным документам по стандартизации, метрологии и сертификации

Информационная система по взаимодействию с ВТО предназначена для взаимодействия с Секретариатом ВТО, международными организациями, предоставления заинтересованным лицам уведомлений, соответствующей документации и информации, касающейся стандартов и процедур оценки соответствия.

4.2 Требования к защите ИС ГФС реализуются в виде совокупности программно-технических средств защиты. Общие требования к программным документам в соответствии с ГОСТ 19.105.

Совокупность всех средств защиты составляет комплекс средств защиты (КСЗ).

4.3 В связи с тем, что показатели защищенности ИС ГФС описываются требованиями, варьируемыми по уровню и глубине, в зависимости от класса защищенности СВТ, в настоящем стандарте для любого показателя приводится набор требований, соответствующий высшему классу защищенности от НСД.

4.4 ИС ГФС должна обеспечить защиту используемой информации в соответствии с требованиями уровня безопасности, в частности:

пересылаемая по внешним каналам информация должна быть защищена с помощью сертифицированных аппаратных или программных криптографических средств;

должно быть обеспечено разграничение прав доступа пользователей к ИС ГФС;

должен быть предотвращен несанкционированный доступ посторонних лиц через телекоммуникационный узел Интернета.

4.5 Безопасность информационных ресурсов должна быть обеспечена встроенными средствами применяемых систем управления БД, оригинальными программными средствами контроля доступа к защищаемой информации, а также соответствующими организационными мерами.

5 Классификация средств защиты информационной системы Государственного фонда стандартов

5.1 Виды технических средств защиты информации

5.1.1 Настоящий стандарт устанавливает следующие виды технических средств защиты информации:

- средства защиты информации от несанкционированного доступа (НСД);
- программное обеспечение для средств защиты информации;
- защищённые программные средства обработки информации;
- программно-технические средства защиты информации.

5.2 Классификация технических средств защиты информации от НСД.

5.2.1 К техническим средствам защиты информации от НСД относятся:

- средства пассивной защиты, в том числе:

а) замки (с управлением от микропроцессора, радиоуправляемые и т.п.);

б) электрические датчики разных видов;

в) телевизионные системы охраны и контроля;

з) кабельные системы;

к) устройства идентификации, ограждения;

л) средства обнаружения нарушителя или нарушающего воздействия;

м) специальные средства для транспортировки и хранения физических носителей информации (кассет стримеров, магнитных и оптических

дисков и т.п).

5.3 Классификация программно-технических средств защиты информации

К программно-техническим средствам защиты информации относятся:

- устройства прерывания программы пользователя при нарушении им правил доступа;
- устройство стирания данных;
- устройство выдачи сигнала тревоги при попытке НСД;
- устройство локализации электронных закладок;
- программно-аппаратные средства разграничения доступа к информации, встроенные в информационные технологии.

5.4 Классификация программных средств защиты информации

К программным средствам защиты информации относятся:

- программы, обеспечивающие разграничение доступа к информации по мандатному, дискреционному или многоуровневому принципам (матрица и диспетчер доступа, электронный журнал доступа пользователей к информации, метки секретности и т.п.);
- программы идентификации и аутентификации терминалов и пользователей по различным признакам (пароль, дополнительное кодовое слово, биометрические данные и т.п.), в том числе программы повышения идентификации (аутентификации);
- программы проверки функционирования системы защиты информации от НСД;
- программы контроля целостности средств защиты;
- программы защиты различного вспомогательного назначения, в том числе и антивирусные программы;
- программы защиты операционных систем персональных электронно-вычислительных машин (модульная программная интерпретация и т.п.);
- программы контроля целостности общесистемного и прикладного программного обеспечения;
- программы, сигнализирующие о нарушении использования ресурсов;
- программы контроля файловой структуры на внешних запоминающих устройствах и средства восстановления;
- программы имитации работы системы или её блокировки при обнаружении фактов НСД;
- программы обнаружения фактов НСД и сигнализации (передачи сообщений) об их обнаружении;
- программы обнаружения и локализации программных закладок;
- тестирующие программы и программы обработки результатов измерений;
- программное обеспечение для защиты от НСД из Интернета

6 Общие технические требования

6.1 Защищенность от НСД к информации при ее обработке СВТ характеризуется тем, что только надлежащим образом уполномоченные лица или процессы, инициированные ими, будут иметь доступ к чтению, записи, созданию или уничтожению информации.

Защищенность обеспечивается тремя группами требований к средствам защиты, реализуемым в СВТ:

а) требования к разграничению доступа, предусматривающие, что СВТ должны поддерживать непротиворечивые, однозначно определенные правила разграничения доступа;

б) требования к учету, предусматривающие, что СВТ должны поддерживать регистрацию событий, имеющих отношение к защищенности информации;

в) требования к гарантиям, предусматривающие необходимость наличия в составе СВТ технических и программных механизмов, позволяющих получить гарантии того, что СВТ обеспечивают выполнение требований к разграничению доступа и к учету.

6.2 Требования к разграничению доступа

6.2.1 Требования к разграничению доступа определяют следующие показатели защищенности, которые должны поддерживаться СВТ

а) дискреционный принцип контроля доступа;

б) мандатный принцип контроля доступа;

в) идентификация и аутентификация;

г) очистка памяти;

д) изоляция модулей;

е) защита ввода и вывода на отчуждаемый физический носитель информации;

ж) сопоставление пользователя с устройством.

6.2.2 Для реализации дискреционного принципа контроля доступа, КСЗ должен контролировать доступ именованных субъектов (пользователей) к именованным объектам (например, файлам, программам, базам данных).

Для каждой пары (субъект — объект) в СВТ должно быть дано явное и недвусмысленное перечисление допустимых типов доступа (например, читать, писать), т.е. тех типов доступа, которые являются санкционированными для данного субъекта индивида или группы индивидов) к данному ресурсу СВТ объекту).

Контроль доступа должен быть применим к каждому объекту каждому субъекту (индивиду или группе равноправных индивидов).

Механизм, реализующий дискреционный принцип контроля ступа, должен предусматривать санкционированное изменение правил разграничения доступа (ПРД), в том числе санкционированное изменение списка пользователей СВТ и списка защищаемых объектов.

Право изменять ПРД должно быть предоставлено выделенным объектам (например, администрации, службе безопасности).

Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

КСЗ должен содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых. Под "явными" здесь подразумеваются действия, осуществляемые с использованием системных средств, под "скрытыми" — иные действия, в том числе с использованием собственных программ .работы с устройствами.

6.2.3 Для реализации мандатного принципа контроля доступа каждому субъекту и каждому объекту присваивают классификационные метки, отражающие их место в соответствующей иерархии. С помощью этих меток субъектам и объектам должны быгь назначены классификационные уровни, являющиеся комбинациями уровня иерархической классификации и иерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.

КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном внесении в список пользователей нового субъекта, ему должны быть назначены классификационные метки. Внешние классификационные метки субъектов (объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

КСЗ должен реализовать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе стороны любого из субъектов:

а) субъект может читать объект, если уровень иерархической классификации в классификационном уровне объекта не меньше, чем уровень иерархической классификации в классификационном уровне субъекта, и иерархические категории в классификационном уровне субъекта включают в себя все неиерархические категории в классификационном уровне объекта:

б) субъект осуществляет запись в объект, если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все неиерархические категории в классификационном уровне субъекта включены в неиерархические категории в классификационном уровне объекта.

Реализация мандатных ПРД должна предусматривать возможности сопровождения — изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

В СВТ должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа, при этом решение о санкционированности запроса на доступ следует принимать только при одновременном разрешении его дискреционными и мандатными ПРД. Таким образом, должен быть контролируемым не только «единичный акт» доступа, но и потоки информации.

6.2.4 КСЗ должен обеспечивать идентификацию субъектов при запросах на доступ, должен проверять подлинность идентификатора субъекта – осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации и препятствовать доступу к защищаемым ресурсам неидентифицированных субъектов или субъектов, чья подлинность при аутентификации не подтвердилась.

КСЗ должен обладать способностью связывать полученный результат идентификации и аутентификации со всеми действиями, относящимися к контролю, предпринимаемыми в отношении данного субъекта.

6.2.5 КСЗ должен осуществлять очистку оперативной и внешней памяти. Очистка должна производиться путем записи маскирующей информации в память при ее освобождении (перераспределении).

6.2.6 При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса от программных модулей других процессов, т.е. в оперативной памяти ЭВМ программы разных пользователей должны быть защищены друг от друга.

6.2.7 КСЗ должен различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или как идентифицированные ("помеченные"). При вводе с "помеченного" устройства (выводе на "помеченное" устройство) КСЗ должен обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно быть при работе с "помеченным" каналом связи.

Изменения в назначении и разметке устройств и каналов должны осуществляться только под контролем КСЗ.

6.2.8 КСЗ должен обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки).

КСЗ должен включать в себя механизм, с помощью которого санкционированный пользователь надежно сопоставляется с выделенным ему идентифицированным устройством.

6.3 Требования к учету

6.3.1 Требования к учету определяют следующие показатели защищенности, которые должны поддерживаться СВТ:

- регистрация;
- маркировка документов.

6.3.2 КСЗ должен осуществлять регистрацию следующих событий:

а) использование идентификационного и аутентификационного механизма;

б) запрос на доступ к защищаемому ресурсу (например, открытие файла, запуск программы);

в) создание и уничтожение объекта;

г) действия, связанные с изменением ПРД. Для каждого из этих событий должна быть зарегистрирована следующая информация:

- дата и врем я;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то отмечают объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

КСЗ должен содержать средства выборочного ознакомления с регист-

рационной информацией.

Для высоких классов защищенности СВТ должна быть предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных субъектов (например, администраторов защиты).

6.3.3 КСЗ должен обеспечивать вывод защищаемой информации на документ вместе с ее классификационной меткой.

6.4 Требования к отказоустойчивости

6.4.1 Требования к отказоустойчивости определяют следующие показатели защищенности, которые должны поддерживаться СВТ:

а) методы резервного копирования;

б) надежное восстановление;

в) целостность КСЗ;

г) контроль модификации;

д) контроль дистрибуции;

е) взаимодействие пользователя с КСЗ;

ж) тестирование.

6.4.2 На начальном этапе проектирования КСЗ должна быть построена модель защиты, задающая принцип разграничения доступа и механизм управления доступом. Эта модель должна содержать:

а) непротиворечивые ПРД;

б) непротиворечивые правила изменения ПРД;

в) правила работы с устройствами ввода и вывода;

г) формальную модель механизма управления доступом.

Спецификация части КСЗ, реализующего механизм управления доступом и его интерфейсов, должна быть высокоуровневой. Эта спецификация должна быть верифицирована на соответствие заданным принципам разграничения доступа.

6.4.3 Процедуры восстановления после сбоев и отказов оборудования должны обеспечивать полное восстановление свойств КСЗ.

6.4.4 В СВТ должны быть предусмотрены средства периодического контроля за целостностью программной и информационной части КСЗ.

Программы КСЗ должны выполняться в отдельной части оперативной памяти. Это требование должно быть подвергнуто верификации.

6.4.5 При проектировании, построении и сопровождении СВТ должно быть предусмотрено управление конфигурацией СВТ, т.е. управление изменениями в формальной модели, спецификациях (разных уровней), документации, исходном тексте, версии в объектном коде. Между документацией и текстами программ должно быть соответствие. Генерируемые версии должны быть сравнимыми. Оригиналы программ должны быть защищены.

6.4.6 При изготовлении копий с оригинала СВТ, должен быть осуществлен контроль точности копирования КСЗ. Изготовленная копия должна гарантированно повторять образец.

6.4.7 КСЗ должен обладать механизмом, гарантирующим перехват диспетчером доступа всех обращений субъектов к объектам.

6.4.8 КСЗ должен иметь модульную и четко определенную структуру, что сделает возможными его изучение, анализ, верификацию и модификацию. Должен быть обеспечен надежный интерфейс пользователя и КСЗ (на-

пример, вход в систему, запросы пользователей и КСЗ). Каждый интерфейс пользователя и КСЗ должен быть логически изолирован от других таких же интерфейсов.

6.4.9 В СВТ должны тестировать:

а) реализация ПРД (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов на доступ, функционирование средств защиты механизма разграничения доступа, санкционированные изменения ПРД и др.);

б) очистка оперативной и внешней памяти;

в) работа механизма изоляции процессов в оперативной памяти;

г) маркировка документов;

д) защита ввода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством;

е) идентификация и аутентификация, а также средства их защиты;

ж) регистрация событий, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;

з) работа механизма надежного восстановления;

и) работа механизма, осуществляющего контроль за целостностью КСЗ;

к) работа механизма, осуществляющего контроль дистрибуции.

7 Требования к документации

7.1 При приемке СВТ, их сертификации и испытаниях других видов необходимо подробное и всестороннее описание КСЗ, т.е. необходима документация, включающая в себя:

а) руководство пользователя;

б) руководство по КСЗ;

в) тестовую документацию;

г) конструкторскую (проектную) документацию.

7.1.1 Руководство пользователя должно включать в себя краткое описание способов использования КСЗ и его интерфейсов с пользователем.

7.1.2 Руководство по КСЗ адресовано администратору защиты и должно содержать:

а) описание контролируемых функций;

б) руководство по генерации КСЗ;

в) описание старта СВТ и процедур проверки правильности старта;

г) описание процедур работы со средствами регистрации;

д) руководство по средствам надежного восстановления;

е) руководство по средствам контроля модификации и дистрибуции.

7.1.3 Тестовая документация должна содержать описание тестов и испытаний, которым подвергались СВТ, а также результатов тестирования.

7.1.4 Конструкторская (проектная) документация должна содержать:

а) общее описание принципов работы СВТ;

б) общую схему КСЗ;

в) описание внешних интерфейсов КСЗ и интерфейсов модулей КСЗ;

г) описание модели защиты;

д) описание диспетчера доступа;

е) описание механизма контроля целостности КСЗ;

ж) описание механизма очистки памяти; з) описание механизма изоляции программ в оперативной памяти;

и) описание средств защиты ввода и вывода на отчуждаемый физический носитель информации и сопоставления пользователя с устройством;

к) описание механизма идентификации и аутентификации;

л) описание средств регистрации;

м) высокоуровневую спецификацию КСЗ и его интерфейсов;

н) верификацию соответствия высокоуровневой спецификации КСЗ модели защиты;

о) описание гарантий проектирования и эквивалентность дискреционных и мандатных ПРД.

УДК 681.32:006354 МКС 35.100

Ключевые слова: средства вычислительной техники, защита от несанкционированного доступа к информации, комплекс средств защиты, требования к средствам защиты