2.5

O‘z DSt 2417:2014

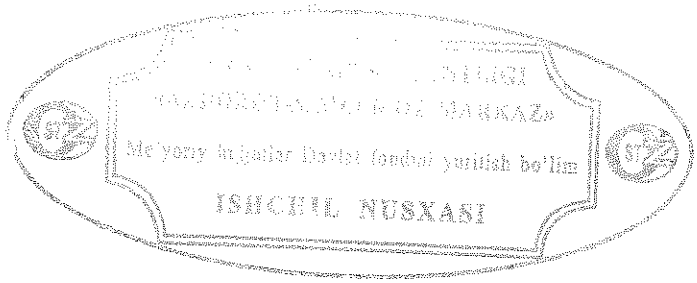
ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Классификация по уровню защищенности от несанкционированного доступа к информации

Издание официальное



Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

O‘z DSt 881:2014

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН Службой национальной безопасности Республики Узбекистан

2 УТВЕРЖДЕН и ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») 18.03.2014 № 05-530

3 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Республики Узбекистан публикуются в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агенством «Узстандарт».

Исключительное право официального опубликования настоящего стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

O'ZBEKISTON RESPUBLIKASI STANDARTLASHTIRISH, METROLOGIYA VA MUVOFIQLIKNI MAZORATINI MUVOFIQLASHTIRISH AXBOROT TEXNOLOGIYALARI VA JORIY ETISH MARKAZI

Содержание

1 Область применения 1

2 Термины, определения и сокращения 1

3 Общие положения 2

4 Требования к показателям шестого класса защищенности 4

5 Требования к показателям пятого класса защищенности 5

6 Требования к показателям четвертого класса защищенности. 8

7 Требования к показателям третьего класса защищенности 12

8 Требования к показателям второго класса защищенности 15

9 Требования к показателям первого класса защищенности 19

10 Оценка класса защищенности СВТ (сертификация СВТ) 21

O‘ZBEKISTON RESPUBLIKASI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси
ҲИСОБЛАШ ТЕХНИКА ВОСИТАЛАРИ
Ахборотдан рухсатсиз фойдалана олишдан муҳофазаланганлик даражалари буйича таснифлаш

Информационная технология
СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ
Классификация по уровню защищенности от несанкционированного доступа к информации

Information technology
Means of calculating techniques
Classification by level of protection from unauthorized access to information

Дата введения 31 03 2015

1 Область применения

Настоящий стандарт устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации в соответствии с показателями защищенности и совокупностью описывающих их требований.

Показатели защищенности средств вычислительной техники применяются к общесистемным программным средствам и операционным системам (с учетом архитектуры ЭВМ).

2 Термины, определения и сокращения

В настоящем стандарте применены следующие термины с соответствующими определениями:

2.1 **внешняя память:** Память, данные в которой доступны центральному процессору посредством операций ввода-вывода.

2.2 **комплекс средств защиты;** КСЗ: Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или систем от несанкционированного доступа к информации.

O'ZSTANDART AGENTLIGI
4201 son olindi
« 24 » 03 2015 yil
Davlat ro'yxatiga olindi

2.3 **несанкционированный доступ;** НСД: Доступ субъекта к объекту или информации в нарушение установленных в системе правил разграничения доступа.

2.4 **остаточная информация:** Информация на запоминающем устройстве, оставшаяся от формально удалённых операционной системой данных или из-за физических свойств запоминающих устройств.

2.5 **правила разграничения доступа;** ПРД: Совокупность правил регламентирующих права доступа к объектам доступа.

3 Общие положения

3.1 Под средствами вычислительной техники (СВТ) понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

3.2 Требования к показателям реализуются с помощью программно-технических средств. Данные показатели содержат требования защищенности СВТ от НСД к информации.

Совокупность всех средств защиты составляет КСЗ.

Документация КСЗ должна быть неотъемлемой частью конструкторской документации (КД) на СВТ.

3.3 Конкретные перечни показателей защищенности СВТ определяют классы защищенности СВТ.

Каждый показатель описывается совокупностью требований.

3.4 СВТ по уровню защищенности от НСД к информации подразделяются на семь классов.

Самый низкий класс - седьмой, самый высокий - первый.

3.5 Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

3.6 Выбор класса защищенности СВТ для автоматизированных систем (АС), создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

3.7 Для повышения гарантий качества защиты в комплекте СВТ возможно применение средств криптографической защиты информации, реализующих алгоритмы, рекомендованные Уполномоченным органом.

[illegible] AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH [illegible]
AXBOROT TEXNOLOGIYALARI
JORIY ETISH BOSHQARMASI

3.8 Перечень показателей по классам защищенности СВТ приведен в таблице 1.

Таблица 1

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	+	+	+
Мандатный принцип контроля доступа	-	-	+	+	+	+
Очистка памяти	-	+	+	+	+	+
Изоляция модулей	-	-	+	+	+	+
Маркировка документов	-	-	+	+	+	+
Защита ввода и вывода на съемный носитель информации	-	-	+	+	+	+
Сопоставление пользователя с устройством	-	-	+	+	+	+
Идентификация и аутентификация	+	+	+	+	+	+
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	+	+
Взаимодействие пользователя с КСЗ	-	-	-	+	+	+
Надежное восстановление	-	-	-	+	+	+
Целостность КСЗ	-	+	+	+	+	+
Контроль модификации	-	-	-	-	+	+
Контроль дистрибуции	-	-	-	-	+	+
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	+
Руководство для пользователя	+	+	+	+	+	+
Руководство по КСЗ	+	+	+	+	+	+
Тестовая документация	+	+	+	+	+	+
Конструкторская (проектная) документация	+	+	+	+	+	+
Примечание - «+» - есть требования к данному классу, «-» - нет требований к данному классу.						

3.9 Приведенные в данном разделе наборы требований к показателям каждого класса являются минимально необходимыми.

3.10 Уменьшение или изменение перечня показателей, соответствующего конкретному классу защищенности СВТ, не допускается.

3.11 Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований шестого класса.

4 Требования к показателям шестого класса защищенности

4.1 Дискреционный принцип контроля доступа

КСЗ должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.).

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

КСЗ должен содержать механизм, реализующий дискреционные правила разграничения доступа.

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

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.

Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).

4.2 Идентификация и аутентификация

КСЗ должен

- требовать от пользователей идентифицировать себя при запросах на доступ;
- подвергать проверке подлинность идентификации - осуществлять аутентификацию;
- располагать необходимыми данными для идентификации и аутентификации;
- препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.

4.3 Тестирование

В СВТ шестого класса должны тестироваться:

- реализация дискреционных ПРД (перехват явных и скрытых запросов, правильное распознавание санкционированных и несанкционированных запросов на доступ, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);
- успешное осуществление идентификации и аутентификации, а также их средств защиты.

...DAVLAT ...

4.4 Руководство для пользователя

Руководство для пользователя должно содержать описание способов использования КСЗ и его интерфейса с пользователем.

4.5 Руководство по КСЗ

Руководство по КСЗ адресовано администратору защиты и должно содержать:

- описание контролируемых функций;
- руководство по настройке КСЗ;
- описание запуска СВТ и процедур тестирования правильности запуска.

4.6 Тестовая документация

Тестовая документация должна содержать описание тестов и испытаний, которым подвергалось, в соответствии с 4.3, СВТ и результатов тестирования.

4.7 Конструкторская (проектная) документация

Конструкторская (проектная) документация должна содержать общее описание принципов работы СВТ, общую схему КСЗ, описание интерфейсов КСЗ с пользователем и интерфейсов частей КСЗ между собой, описание механизмов идентификации и аутентификации.

5 Требования к показателям пятого класса защищенности

5.1 Дискреционный принцип контроля доступа

Требования аналогичны требованиям шестого класса, приведенным в 4.1, и дополнительно должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

5.2 Очистка памяти

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации.

STANDARTLASHTIRISH, DAVLAT
MUVOFIQLASHTIRISH VA
TEXNOLOGIYALARGA

5.3 Идентификация и аутентификация

Требования аналогичны требованиям шестого класса, приведенным в 4.2.

5.4 Гарантии проектирования

На начальном этапе проектирования СВТ должна быть построена модель защиты. Модель должна включать в себя ПРД к объектам и непротиворечивые правила изменения ПРД.

5.5 Регистрация

КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

– использование идентификационного и аутентификационного механизма;

– запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);

– создание и уничтожение объекта;

– действия по изменению ПРД.

Для каждого из этих событий должна регистрироваться следующая информация:

– дата и время;

– субъект, осуществляющий регистрируемое действие;

– тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);

– успешно ли осуществилось событие (обслужен запрос на доступ или нет).

КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией.

5.6 Целостность КСЗ

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

5.7 Тестирование

В СВТ пятого класса защищенности должны тестироваться:

– реализация ПРД (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных

O'ZSTANDART AGE
STANDARTLA
NAZORATINI
AXBOROT

запросов, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);

– успешное осуществление идентификации и аутентификации, а также их средства защиты;

– очистка памяти в соответствии с 5.2;

– регистрация событий в соответствии с 5.5, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;

– работа механизма, осуществляющего контроль за целостностью КСЗ.

5.8 Руководство пользователя

Требования аналогичны требованиям шестого класса, приведенным в 4.4.

5.9 Руководство по КСЗ

Руководство по КСЗ адресовано администратору защиты и должно содержать:

– описание контролируемых функций;

– руководство по настройке КСЗ;

– описание запуска СВТ и процедур тестирования правильности запуска, процедур работы со средствами регистрации.

5.10 Тестовая документация

Тестовая документация должна содержать описание тестов и испытаний, которым подвергалось СВТ в соответствии с требованиями 5.7, и результатов тестирования.

5.11 Конструкторская и проектная документация

Конструкторская и проектная документация должна содержать:

– описание принципов работы СВТ;

– общую схему КСЗ;

– описание интерфейсов КСЗ с пользователем и интерфейсов модулей КСЗ;

– модель защиты;

– описание механизмов контроля целостности КСЗ, очистки памяти, идентификации и аутентификации.

O'ZBEKISTON STANDARTLARI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

6 Требования к показателям четвертого класса защищенности.

6.1 Дискреционный принцип контроля доступа

Требования аналогичны требованиям пятого класса, приведенным в 5.1.

Дополнительно КСЗ должен содержать механизм, реализующий дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, не допустимого с точки зрения заданного ПРД). Под «явными» подразумеваются действия, осуществляемые с использованием системных средств - системных макрокоманд, инструкций языков высокого уровня и т.д., а под «скрытыми» - иные действия, в том числе с использованием собственных программ работы с устройствами.

Дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД.

6.2 Мандатный принцип контроля доступа

Для реализации этого принципа должна производиться проверка соответствия официального разрешения (допуска) каждого субъекта и метки конфиденциальности каждого объекта, отражающие их место в соответствующей иерархии. Посредством официальных разрешений (допусков) субъектам и меток конфиденциальности объектам должны назначаться классификационные уровни по уровням уязвимости, категориям секретности и т.п.

КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя метки конфиденциальности этих данных. При санкционированном занесении в список пользователей нового субъекта должно производиться соответствие ему официального разрешения (допуска).

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

- субъект может читать информацию из объекта, если классификационный уровень субъекта не ниже, чем у объекта, а все категории, перечисленные в метке конфиденциальности объекта, присутствуют в официальном разрешении (допуске) субъекта;

- субъект может записывать информацию в объект, если метка конфиденциальности объекта доминирует над официальным разрешением (допуском) субъекта.

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

O'ZBEKISTON RESPUBLIKASI DAVLAT STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

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 должно приниматься только при одновременном разрешении его дискреционными и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

6.3 Очистка памяти

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен затруднять субъекту доступ к остаточной информации. При перераспределении оперативной памяти КСЗ должен осуществлять ее очистку.

6.4 Изоляция модулей

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

6.5 Маркировка документов.

6.5.1 Для документированных материалов

При выводе защищаемой информации на бумажный носитель в начале и конце проставляют штамп и заполняют его реквизиты согласно соответствующей инструкции.

6.5.2 Для электронных документов

В электронном документе основным реквизитом является наличие электронно цифровой подписи согласно законодательству Республики Узбекистан.

6.6 Защита ввода и вывода на съемный носитель информации

КСЗ должен различать каждое устройство ввода-вывода как произвольно используемые или идентифицированные. При вводе с идентифицированного устройства (вывода на идентифицированное устройство) КСЗ должен обеспечивать соответствие между меткой

конфиденциальности вводимого (выводимого) объекта (классификационным уровнем) и меткой конфиденциальности устройства.

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

6.7 Сопоставление пользователя с устройством

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

Идентифицированный КСЗ должен включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству.

6.8 Идентификация и аутентификация

КСЗ должен:

- требовать от пользователей идентифицировать себя при запросах на доступ;
- проверять подлинность идентификатора субъекта - осуществлять аутентификацию;
- располагать необходимыми данными для идентификации и аутентификации и препятствовать входу в СВТ не идентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась;
- обладать способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя.

6.9 Гарантии проектирования

Проектирование КСЗ должно начинаться с построения модели защиты, содержащей:

– непротиворечивые ПРД;
– непротиворечивые правила изменения ПРД;
– требования для работы с устройствами ввода и вывода информации и каналами связи.

6.10 Регистрация

Требования аналогичны требованиям пятого класса защищенности, приведенным в 5.5.

Дополнительно должна быть предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.).

O'ZBEKISTON AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARI
JORIY ETISH BO'LIMI

6.11 Целостность КСЗ

В СВТ четвертого класса защищенности должен осуществляться периодический контроль за целостностью КСЗ.

Программы КСЗ должны выполняться в отдельной части оперативной памяти.

6.12 Тестирование

В четвертом классе защищенности должны тестироваться:

– реализация ПРД (перехват запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов в соответствии с дискреционными и мандатными правилами, верное сопоставление меток субъектов и объектов, запрос меток вновь вводимой информации, средства защиты механизма разграничения доступа, санкционированное изменение ПРД);

– невозможность присвоения субъектом себе новых прав;

– очистка оперативной и внешней памяти;

– работа механизма изоляции процессов в оперативной памяти;

– маркировка документов;

– защита ввода и вывода информации на съемный физический носитель и сопоставление пользователя с устройством;

– идентификация и аутентификация, а также их средства защиты;

– запрет на доступ несанкционированного пользователя;

– работа механизма, осуществляющего контроль за целостностью СВТ;

– регистрация событий, описанных в 6.10, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией.

6.13 Руководство для пользователя

Требования аналогичны требованиям шестого класса, приведенным в 4.4.

6.14 Руководство по КСЗ

Требования аналогичны требованиям пятого класса, приведенным в 5.9.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

6.15 Тестовая документация

Тестовая документация должна содержать описание тестов и испытаний, которым подвергалось СВТ в соответствии с 6.12, и результатов тестирования.

6.16 Конструкторская (проектная) документация

Конструкторская (проектная) документация должна содержать:

- общее описание принципов работы СВТ;
- общую схему КСЗ;
- описание внешних интерфейсов КСЗ и интерфейсов модулей КСЗ;
- описание модели защиты;
- описание диспетчера доступа;
- описание механизма контроля целостности КСЗ;
- описание механизма очистки памяти;
- описание механизма изоляции программ в оперативной памяти;
- описание средств защиты ввода и вывода на съемный физический носитель информации и сопоставления пользователя с устройством;
- описание механизма идентификации и аутентификации;
- описание средств регистрации.

7 Требования к показателям третьего класса защищенности

7.1 Дискреционный принцип контроля доступа

Требования аналогичны требованиям пятого и четвертого классов, приведенных в 5.1 и 6.1 соответственно.

7.2 Мандатный принцип контроля доступа

Требования аналогичны требованиям четвертого класса, приведенным в 6.2.

7.3 Очистка памяти

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

7.4 Изоляция модулей

Требования аналогичны требованиям четвертого класса, приведенным в 6.4.

7.5 Маркировка документов

Требования аналогичны требованиям четвертого класса, приведенным в 6.5.

7.6 Защита ввода и вывода на съемный физический носитель информации

Требования аналогичны требованиям четвертого класса, приведенным в 6.6.

7.7 Сопоставление пользователя с устройством

Требования аналогичны требованиям четвертого класса, приведенным в 6.7.

7.8 Идентификация и аутентификация

Требования аналогичны требованиям четвертого класса, приведенным в 6.8.

7.9. Гарантии проектирования

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

– непротиворечивые правила изменения ПРД;

– требования для работы с устройствами ввода и вывода информации и каналами связи;

– формальную модель механизма управления доступом.

Должна предлагаться высокоуровневая спецификация части КСЗ, реализующего механизм управления доступом и его интерфейсов. Эта спецификация должна быть верифицирована на соответствие заданных принципов разграничения доступа.

7.10 Регистрация

Требования аналогичны требованиям четвертого класса, приведенным в 6.10.

...AGENTLIGI
...LASHTIRISH, DAVLAT
...MUVOFIQLASHTIRISH VA
...TEXNOLOGIYALARINI
...ETISH BOSHQARMASI

7.11 Взаимодействие пользователя с КСЗ

Для обеспечения возможности изучения, анализа, верификации и модификации КСЗ должен быть хорошо структурирован, его структура должна быть модульной и четко определенной. Интерфейс пользователя и КСЗ должен быть определен (вход в систему, запросы пользователей и КСЗ и т.п.). Должна быть обеспечена надежность такого интерфейса. Каждый интерфейс пользователя и КСЗ должен быть логически изолирован от других таких же интерфейсов.

7.12 Надежное восстановление

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

7.13 Целостность КСЗ

Необходимо осуществлять периодический контроль за целостностью КСЗ.

Программы должны выполняться в отдельной части оперативной памяти. Это требование должно подвергаться верификации.

7.14 Тестирование

СВТ должны подвергаться такому же тестированию, что и СВТ четвертого класса в соответствии с 6.12.

Дополнительно должны тестироваться:

- очистка памяти по 7.3;
- работа механизма надежного восстановления.

7.15 Руководство для пользователя

Требования аналогичны требованиям четвертого класса, приведенным в 6.13.

7.16 Руководство по КСЗ

Руководство по КСЗ адресовано администратору защиты и должно содержать:

- описание контролируемых функций;
- руководство по настройке КСЗ;
- описание запуска СВТ и процедур тестирования правильности запуска, процедур работы со средствами регистрации;
- руководство по средствам надежного восстановления.

O'ZBEKISTON STANDARTLASHTIRISH MILLIY AXBOROT

7.17 Тестовая документация

Тестовая документация должна содержать описание тестов и испытаний, которым подвергалось СВТ в соответствии с 7.14, а также результатов тестирования.

7.18 Конструкторская (проектная) документация.

Требования аналогичны требованиям четвертого класса, приведенным в 6.16. Дополнительно необходимы:

- детальная спецификация КСЗ и его интерфейсов;
- верификация соответствия высокоуровневой спецификации КСЗ модели защиты.

8 Требования к показателям второго класса защищенности

8.1 Дискреционный принцип контроля доступа

Требования аналогичны требованиям третьего класса, приведенным в 7.1.

Дополнительно требуется, чтобы дискреционные правила разграничения доступа были эквивалентны мандатным правилам (т.е. всякий запрос на доступ должен быть одновременно санкционированным или несанкционированным одновременно и по дискреционным правилам, и по мандатным ПРД).

8.2 Мандатный принцип контроля доступа

Требования аналогичны требованиям третьего класса, приведенным в 7.2.

8.3. Очистка памяти

Требования аналогичны требованиям третьего класса, приведенным в 7.3.

8.4 Изоляция модулей

Требования аналогичны требованиям третьего класса, приведенным в 7.4.

Дополнительно гарантии изоляции должны быть основаны на архитектуре СВТ.

STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARI
JORIY ETISH BOSHQAR ASI

8.5 Маркировка документов

Требования аналогичны требованиям третьего класса, приведенным в 7.5.

8.6 Защита ввода и вывода на съемный физический носитель информации

Требования аналогичны требованиям третьего класса, приведенным в 7.6.

8.7 Сопоставление пользователя с устройством

Требования аналогичны требованиям четвертого и третьего классов, приведенным в 6.7 и 7.7 соответственно.

8.8 Идентификация и аутентификация

Требования аналогичны требованиям четвертого и третьего классов, приведенным в 6.8 и 7.8 соответственно.

8.9 Гарантии проектирования

Требования аналогичны требованиям третьего класса, приведенным в 7.9.

Дополнительно требуется, чтобы высокоуровневые спецификации КСЗ были отображены последовательно в спецификации одного или нескольких нижних уровней, вплоть до реализации высокоуровневой спецификации КСЗ на языке программирования высокого уровня. При этом методами верификации должно осуществляться доказательство соответствия каждого такого отображения спецификациям высокого (верхнего для данного отображения) уровня. Этот процесс может включать в себя как одно отображение (высокоуровневая спецификация - язык программирования), так и последовательность отображений в промежуточные спецификации с понижением уровня, вплоть до языка программирования. В результате верификации соответствия каждого уровня предыдущему должно достигаться соответствие реализации высокоуровневой спецификации КСЗ модели защиты, представленной на рисунке 1.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

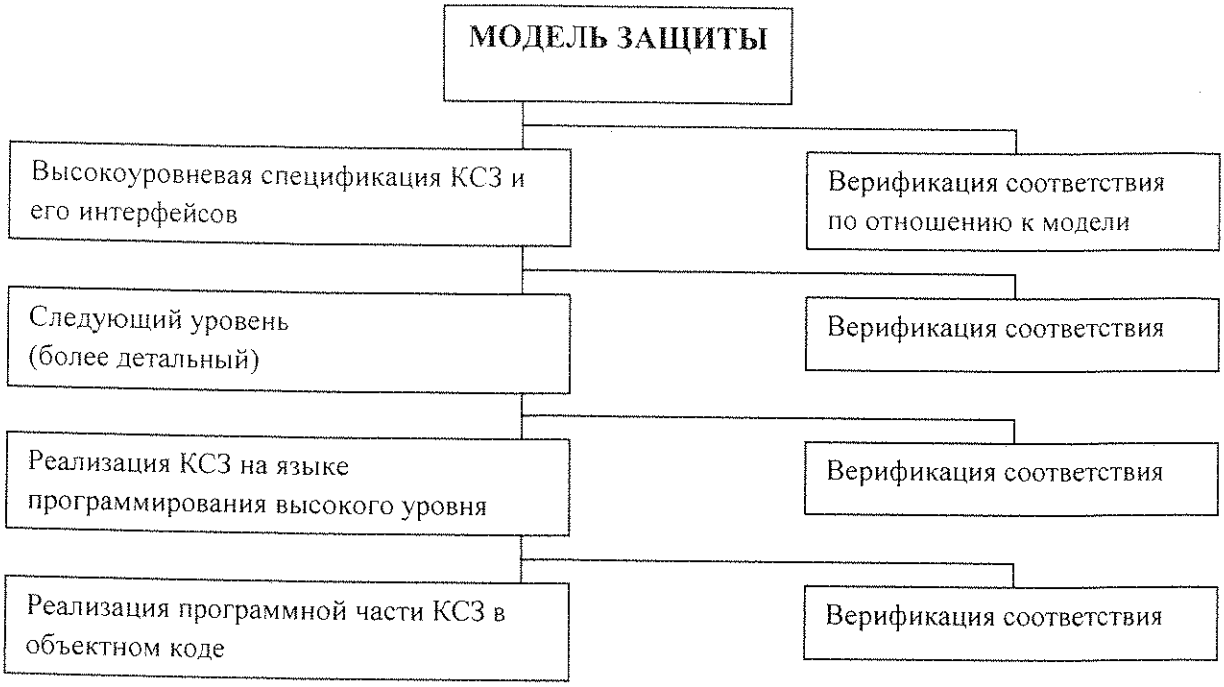


Рисунок 1 - Схема модели защиты

8.10 Регистрация

Требования аналогичны требованиям четвертого и третьего классов, приведенным в 6.10 и 7.10 соответственно.

8.11 Взаимодействие пользователя с КСЗ

Требования аналогичны требованиям третьего класса, приведенным в 7.11.

8.12 Надежное восстановление

Требования аналогичны требованиям третьего класса, приведенным в 7.12.

8.13 Целостность КСЗ

Требования аналогичны требованиям третьего класса, приведенным в 7.13.

8.14 Контроль модификации

При проектировании, построении и сопровождении СВТ должно быть предусмотрено управление конфигурацией СВТ, т.е. контроль изменений в формальной модели, спецификациях (разных уровней), документации, исходном тексте, версии в объектном коде. Должно

...TLASHTIRISH DAVLAT ...LASHTIRISH VA ...TALABLARI

обеспечиваться соответствие между документацией и текстами программ. Должна осуществляться сравниваемость генерируемых версий. Оригиналы программ должны быть защищены.

8.15 Контроль дистрибуции

Должен осуществляться контроль точности копирования в СВТ при изготовлении копий с образца. Изготовляемая копия должна гарантированно повторять образец.

8.16. Тестирование

Требования аналогичны требованиям третьего класса, приведенным в 7.14.

Дополнительно должен тестироваться контроль дистрибуции.

8.17 Руководство для пользователя

Требования аналогичны требованиям четвертого и третьего классов, приведенным в 6.13 и 7.15 соответственно.

8.18 Руководство по КСЗ

Требования аналогичны требованиям третьего класса, приведенным в 7.16.

Дополнительно должны быть представлены руководства по надежному восстановлению, по работе со средствами контроля модификации и дистрибуции.

8.19 Тестовая документация

Тестовая документация должна содержать описание тестов и испытаний, которым подвергалось СВТ в соответствии с 8.16, а также результатов тестирования.

8.20 Конструкторская (проектная) документация

Требования аналогичны требованиям третьего класса, приведенным в 7.18.

Дополнительно должны быть описаны гарантии процесса проектирования и эквивалентность дискреционных по 8.1 и мандатных по 8.2 ПРД.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH ... T
NAZORATINI MUVOFIQLASHTIRISH ... VA
AXBOROT TEXNOLOGIYALARI
JORIY ETILISH BOSQICHI

9 Требования к показателям первого класса защищенности

9.1 Дискреционный принцип контроля доступа

Требования аналогичны требованиям второго класса, приведенным в 8.1.

9.2 Мандатный принцип контроля доступа

Требования аналогичны требованиям второго класса, приведенным в 8.2.

9.3 Очистка памяти

Требования аналогичны требованиям второго класса, приведенным в 8.3.

9.4 Изоляция модулей

Требования аналогичны требованиям второго класса, приведенным в 8.4.

9.5 Маркировка документов

Требования аналогичны требованиям второго класса, приведенным в 8.5.

9.6 Защита ввода и вывода на съемный физический носитель информации

Требования аналогичны требованиям второго класса, приведенным в 8.6.

9.7 Сопоставление пользователя с устройством

Требования аналогичны требованиям второго класса, приведенным в 8.7.

9.8 Идентификация и аутентификация

Требования аналогичны требованиям второго класса, приведенным в 8.8.

9.9 Гарантии проектирования

Требования аналогичны требованиям второго класса, приведенным в 8.9.

Дополнительно требуется верификация соответствия объектного кода тексту КСЗ на языке высокого уровня.

9.10 Регистрация

Требования аналогичны требованиям второго класса, приведенным в 8.10.

9.11 Взаимодействие пользователя с КСЗ

Требования аналогичны требованиям второго класса, приведенным в 8.11.

9.12. Надежное восстановление

Требования аналогичны требованиям второго класса, приведенным в 8.12.

9.13 Целостность КСЗ

Требования аналогичны требованиям второго класса, приведенным в 8.13.

9.14 Контроль модификации

Требования аналогичны требованиям второго класса, приведенным в 8.14.

9.15 Контроль дистрибуции

Требования аналогичны требованиям второго класса, приведенным в 8.15.

9.16 Гарантии архитектуры

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

O‘ZSTANDART AGENTLIGI
STANDARTLA
NAZORATINI
AXBOROT

9.17 Тестирование

Требования аналогичны требованиям второго класса, приведенным в 8.16.

9.18 Руководство пользователя

Требования аналогичны требованиям второго класса, приведенным в 8.17.

9.19 Руководство по КСЗ

Требования аналогичны требованиям второго класса, приведенным в 8.18.

9.20 Тестовая документация

Требования аналогичны требованиям второго класса, приведенным в 8.19.

9.21 Конструкторская (проектная) документация

Требования аналогичны требованиям второго класса, приведенным в 8.20.

Дополнительно разрабатывается описание гарантий процесса проектирования приведенным в 9.9.

10 Оценка класса защищенности СВТ (сертификация СВТ)

Оценка класса защищенности СВТ проводится по соответствующему положению, а также другим нормативно-правовым актам.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQAR ASI

УДК 004.056.53 ОКС 35.040 П 89

Ключевые слова: средства вычислительной техники, класс защищенности, несанкционированный доступ, дискреционный принцип контроля доступа, мандатный принцип контроля доступа

O‘zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Сотрудник Службы
национальной безопасности
Республики Узбекистан — Д. Мажидов
12.03.2014

Нормоконтроль — Л. Шаймарданова
12.03.2014

СОГЛАСОВАНО

Государственный комитет
связи, информатизации и
телекоммуникационных
технологий Республики
Узбекистан

письмо от 26.02.2014
№ 14-8/1125

O‘ZBEKISTON AXBOROT
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI