ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Средства вычислительной техники

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Общие технические требования

Издание официальное

ГОССТАНДАРТ РОССИИ
Москва

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН Научно-исследовательским институтом "Квант" Главного управления радиопромышленности Комитета по оборонным отраслям промышленности

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 9 февраля 1995 г. № 49

3 ВВЕДЕН ВПЕРВЫЕ

4 ПЕРЕИЗДАНИЕ. Август 2006 г.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Средства вычислительной техники

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Общие технические требования

Computers technique. Information protection against unauthorised access to information. General technical requirements

Дата введения 1996—01—01

1 Область применения

Настоящий стандарт устанавливает единые функциональные требования к защите средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) к информации; к составу документации на эти средства, а также номенклатуру показателей защищенности СВТ, описываемых совокупностью требований к защите и определяющих классификацию СВТ по уровню защищенности от НСД к информации.

Под СВТ в данном стандарте понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

Требования настоящего стандарта являются обязательными.

2 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения:
- СВТ — средства вычислительной техники;
- НСД — несанкционированный доступ;
- КСЗ — комплекс средств защиты;
- ПРД — правила разграничения доступа.

3 Общие положения

3.1 Требования к защите реализуются в СВТ в виде совокупности программно-технических средств защиты.

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

3.2 В связи с тем, что показатели защищенности СВТ 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.

3.3 Стандарт следует использовать при разработке технических заданий, при формулировании и проверке требований к защите информации.

4 Технические требования

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.

Издание официальное

★

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

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

б) требования к учету, предусматривающие то, 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.

5 Группы требований

5.1 Требования к разграничению доступа

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

а) дискретизационный 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.

5.1.2 Для реализации дискретизационного принципа контроля доступа КСЗ должен контролировать доступ именованных субъектов (пользователей) к именованным объектам (например, файлам, программам, томам).

Для каждой пары (субъект — объект) в СВТ должно быть задано 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 и каждому субъекту (индивиду или группе равноправных индивидов).

Механизм, реализующий дискретизационный принцип контроля доступа, 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 субъектам (например, администрации, службе безопасности).

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

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

5.1.3 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 быть 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 со стороны любого из субъектов:

а) субъект может читать объект, если уровень иерархической классификации в классификационном уровне субъекта не меньше, чем уровень иерархической классификации в классификацион-

ном уровне субъекта, и неиерархические 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 дискретизационными и мандатными ПРД. Таким образом, должны быть контролируемыми не только единичный акт доступа, но и потоки информации.

5.1.4 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.

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

5.1.6 При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический 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.

5.1.7 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.

5.1.8 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.

5.2 Требования к учету

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

- регистрация;
- маркировка документов.

5.2.2 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 время;
- 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 регистрационной информацией.

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

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

5.3 Требования к гарантиям

5.3.1 Требования к гарантиям определяют следующие показатели защищенности, которые должны поддерживаться СВТ:

а) гарантии проектирования;

б) надежное восстановление;

в) целостность КСЗ;

г) контроль модификации;

д) контроль дистрибуции;

е) гарантии архитектуры;

ж) взаимодействие пользователя с КСЗ;

з) тестирование.

5.3.2 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.

Для высоких классов защищенности СВТ должно быть предусмотрено, 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 быть доказано соответствие каждого такого отображения спецификациям высокого (верхнего для данного отображения) уровня, а также соответствие объектного кода тексту КСЗ на языке высокого 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.

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

5.3.4 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.

5.3.5 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.

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

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

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

5.3.9 В СВТ должны тестироваться:

а) реализация ПРД (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов на доступ, фуционирование 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.

6 Требования к документации

6.1 Приведенные в разделе 4 показатели определяют качество защиты СВТ от НСД к информации. Однако для подтверждения этого качества 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.
6.1.1 Руководство пользователя должно включать в себя краткое описание способов использования КСЗ и его интерфейсов с пользователем.
6.1.2 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.
6.1.3 Тестовая документация должна содержать описание тестов и испытаний, которым подвергались СВТ, а также результатов тестирования.
6.1.4 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 (по 5.3.2) и эквивалентность дискретизационных и мандатных ПРД.

УДК 681.32:006.354 ОКС 35.020 П85 ОКСТУ 4000

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

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *Р.А. Ментова*
Компьютерная верстка *Л.А. Круговой*

Подписано в печать 31.08.2006. Формат 60×84⅛. Бумага офсетная. Гарнитура Таймс. Печать офсетная.
Усл. печ. л. 0,93. Уч.-изд. л. 0,70. Тираж 53 экз. Зак. 616. С 3230.

ФГУП «Стандартинформ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «Стандартинформ» на ПЭВМ.
Отпечатано в филиале ФГУП «Стандартинформ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.