ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Руководящий документ

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Часть 1. Программное обеспечение средств защиты информации

Классификация по уровню контроля отсутствия недекларированных возможностей

Введен в действие
Приказом Председателя
Гостехкомиссии России
№ 114 от 4.06.99 г.

Москва – 1999

Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации». – М.: ГТК РФ, 1999. – 11 с.

Настоящий Руководящий документ (РД) устанавливает классификацию программного обеспечения (ПО) (как отечественного, так и импортного производства) средств защиты информации (СЗИ), в том числе и встроенных в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недекларированных возможностей.

Действие документа не распространяется на программное обеспечение средств криптографической защиты информации.

Уровень контроля определяется выполнением заданного настоящим РД набора требований, предъявляемого: к составу и содержанию документации, представляемой заявителем для проведения испытаний ПО СЗИ; к содержанию испытаний.

Руководящий документ разработан в дополнение РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», М., Военное издательство, 1992 г., РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», М., Военное издательство, 1992 г. и РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», М., 1997 г.

Документ предназначен для специалистов испытательных лабораторий, заказчиков, разработчиков ПО СЗИ при его контроле в части отсутствия недекларированных возможностей.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Классификация распространяется на ПО, предназначенное для защиты информации ограниченного доступа.

1.2. Устанавливается четыре уровня контроля отсутствия недекларированных возможностей. Каждый уровень характеризуется определенной минимальной совокупностью требований.

1.3. Для ПО, используемого при защите информации, **отнесенной к государственной тайне,** должен быть обеспечен уровень контроля не ниже **третьего**.

1.4. Самый высокий уровень контроля – **первый,** достаточен для ПО, используемого при защите информации с грифом «ОВ».

≥Второй уровень контроля достаточен для ПО, используемого при защите информации с грифом «СС».

≥Третий уровень контроля достаточен для ПО, используемого при защите информации с грифом «С».

1.5 Самый низкий уровень контроля - **четвертый**, достаточен для ПО, используемого при защите **конфиденциальной** информации.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Недекларированные возможности - функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации. Реализацией недекларированных возможностей, в частности, являются программные закладки.

2.6.Фактический маршрут выполнения функциональных объектов – последовательность фактически выполняемых функциональных объектов при определённых условиях (входных данных).

3. ТРЕБОВАНИЯ К УРОВНЮ КОНТРОЛЯ

Таблица 1

№	Наименование требования	Уровень контроля			
		4	3	2	1
	Требования к документации				
1	Контроль состава и содержания документации				
1.1.	Спецификация (ГОСТ 19.202-78)	+	=	=	=
1.2.	Описание программы (ГОСТ 19.402-78)	+	=	=	=
1.3.	Описание применения (ГОСТ 19.502-78)	+	=	=	=
1.4.	Пояснительная записка (ГОСТ 19.404-79)	-	+	=	=
1.5.	Тексты программ, входящих в состав ПО (ГОСТ 19.401-78)	+	=	=	=
	Требования к содержанию испытаний				
2.	Контроль исходного состояния ПО	+	=	=	=
3.	Статический анализ исходных текстов программ				
3.1.	Контроль полноты и отсутствия избыточности исходных текстов	+	+	+	=
3.2.	Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду	+	=	=	+
3.3.	Контроль связей функциональных объектов по управлению	-	+	=	=
3.4.	Контроль связей функциональных объектов по информации	-	+	=	=
3.5.	Контроль информационных объектов	-	+	=	=
3.6.	Контроль наличия заданных конструкций в исходных текстах	-	-	+	+
3.7.	Формирование перечня маршрутов выполнения функциональных объектов	-	+	+	=
3.8.	Анализ критических маршрутов выполнения функциональных объектов	-	-	+	=
3.9.	Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т.п., построенных по исходным текстам контролируемого ПО	-	-	+	=
4.	Динамический анализ исходных текстов программ				

4.1.	Контроль выполнения функциональных объектов	-	+	+	=
4.2.	Сопоставление фактических маршру-тов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа	-	+	+	=
5.	Отчетность	+	+	+	+

Обозначения:

«-» - нет требований к данному уровню;

«+» - новые или дополнительные требования;

«=» - требования совпадают с требованиями предыдущего уровня.

3.2. Требования к четвертому уровню контроля

3.2.1.Контроль состава и содержания документации

В состав документации, представляемой заявителем, должны входить:

Спецификация **(ГОСТ 19.202-78)**, содержащая сведения о составе ПО и документации на него;

Описание программы **(ГОСТ 19.402-78)**, содержащее основные сведения о составе (с указанием контрольных сумм файлов, входящих в состав ПО), логической структуре и среде функционирования ПО, а также описание методов, приемов и правил эксплуатации средств технологического оснащения при создании ПО;

Описание применения **(ГОСТ 19.502-78)**, содержащее сведения о назначении ПО, области применения, применяемых методах, классе решаемых задач, ограничениях при применении, минимальной конфигурации технических средств, среде функционирования и порядке работы.

Исходные тексты программ **(ГОСТ 19.401-78)**, входящих в состав ПО.

Для ПО импортного производства состав документации может отличаться от требуемого, однако содержание должно соответствовать требованиям указанных ГОСТ. **3.2.2. Контроль исходного состояния ПО**

Контроль заключается в фиксации исходного состояния ПО и сравнении полученных результатов с приведенными в документации.

Результатами контроля исходного состояния ПО должны быть рассчитанные уникальные значения контрольных сумм загрузочных модулей и исходных текстов программ, входящих в состав ПО.

Контрольные суммы должны рассчитываться для каждого файла, входящего в состав ПО.

3.2.3. Статический анализ исходных текстов программ

Статический анализ исходных текстов программ должен включать следующие технологические операции:

контроль полноты и отсутствия избыточности исходных текстов ПО на уровне файлов;

контроль соответствия исходных текстов ПО его объектному (загрузочному) коду.

3.2.4. Отчетность

По окончании испытаний оформляется отчет (протокол), содержащий результаты:

контроля исходного состояния ПО;

контроля полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне файлов;

контроля соответствия исходных текстов ПО его объектному (загрузочному) коду.

3.3.Требования к третьему уровню контроля

3.3.1.Контроль состава и содержания документации

Требования полностью включают в себя аналогичные требования к четвертому уровню контроля.

Кроме того, должна быть представлена «Пояснительная записка» (ГОСТ 19.404-79), содержащая основные сведения о назначении компонентов, входящих в состав ПО, параметрах обрабатываемых наборов данных (подсхемах баз данных), формируемых кодах возврата, описание

используемых переменных, алгоритмов функционирования и т.п.

3.3.2.Контроль исходного состояния ПО

Требования полностью включают в себя аналогичные требования к четвёртому уровню контроля.

3.3.3.Статический анализ исходных текстов программ

Кроме аналогичных требований, предъявляемых к четвёртому уровню контроля, дополнительно предъявляются следующие требования:

контроль полноты и отсутствия избыточности исходных текстов ПО на уровне функциональных объектов (процедур);

контроль связей функциональных объектов (модулей, процедур, функций) по управлению;

контроль связей функциональных объектов (модулей, процедур, функций) по информации;

контроль информационных объектов различных типов (например, локальных переменных, глобальных переменных, внешних переменных и т.п.);

формирование перечня маршрутов выполнения функциональных объектов (процедур, функций).

3.3.4. Динамический анализ исходных текстов программ

Динамический анализ исходных текстов программ должен включать следующие технологические операции:

контроль выполнения функциональных объектов (процедур, функций);

сопоставление фактических маршрутов выполнения функциональных объектов (процедур, функций) и маршрутов, построенных в процессе проведения статического анализа.

3.3.5. Отчетность

Кроме аналогичных требований, предъявляемых к четвертому уровню контроля, дополнительно отчет (протокол) должен содержать результаты:

контроля полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне функциональных объектов (процедур);

контроля связей функциональных объектов (модулей, процедур, функций) по управлению;

контроля связей функциональных объектов (модулей, процедур, функций) по информации;

контроля информационных объектов различных типов (например, локальных переменных, глобальных переменных, внешних переменных и т.п.);

формирования перечня маршрутов выполнения функциональных объектов (процедур, функций);

контроля выполнения функциональных объектов (процедур, функций);

сопоставления фактических маршрутов выполнения функциональных объектов (процедур, функций) и маршрутов, построенных в процессе проведения статического анализа.

3.4. Требования ко второму уровню контроля

3.4.1.Контроль состава и содержания документации

Требования полностью включают в себя аналогичные требования к третьему уровню контроля.

3.4.2.Контроль исходного состояния ПО

Требования полностью включают в себя аналогичные требования к третьему уровню контроля.

3.4.3. Статический анализ исходных текстов программ

Кроме аналогичных требований, предъявляемых к третьему уровню контроля, дополнительно предъявляются следующие требования:

контроль полноты и отсутствия избыточности исходных текстов контролируемого программного обеспечения на уровне функциональных объектов (функций);

синтаксический контроль наличия заданных конструкций в

исходных текстах ПО из списка (базы) потенциально опасных программных конструкций;

формирование перечня маршрутов выполнения функциональных объектов (ветвей);

анализ критических маршрутов выполнения функциональных объектов (процедур, функций) для заданных экспертом списков информационных объектов.

построение по исходным текстам контролируемого ПО блок-схем, диаграмм и т.п., и последующий сравнительный анализ алгоритма работы функциональных объектов (процедур, функций) и алгоритма работы, приведенного в “Пояснительной записке”.

3.4.4. Динамический анализ исходных текстов программ

Кроме аналогичных требований, предъявляемых к третьему уровню контроля, дополнительно предъявляются следующие требования:

контроль выполнения функциональных объектов (ветвей);

сопоставление фактических маршрутов выполнения функциональных объектов (ветвей) и маршрутов, построенных в процессе проведения статического анализа

3.4.5 Отчетность

Кроме аналогичных требований, предъявляемых к третьему уровню контроля, дополнительно отчет (протокол) должен содержать результаты:

контроля полноты и отсутствия избыточности исходных текстов контролируемого программного обеспечения на уровне функциональных объектов (функций);

синтаксического контроля наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных конструкций;

формирования перечня маршрутов выполнения функциональных объектов (ветвей);

анализа критических маршрутов выполнения функциональных

объектов (процедур, функций) для заданных экспертом списков информационных объектов;

построения по исходным текстам контролируемого ПО блок-схем, диаграмм и т.п., и последующего сравнительного анализа алгоритма работы функциональных объектов (процедур, функций) и алгоритма работы, приведённого в “Пояснительной записке”;

контроля выполнения функциональных объектов (ветвей);

сопоставления фактических маршрутов выполнения функциональных объектов (ветвей) и маршрутов, построенных в процессе проведения статического анализа.

3.5. Требования к первому уровню контроля

3.5.1. **Контроль состава и содержания документации**

Требования полностью включают в себя аналогичные требования ко второму уровню контроля.

3.5.2. Контроль исходного состояния ПО

Требования полностью включают в себя аналогичные требования ко второму уровню контроля.

3.5.3. Статический анализ исходных текстов программ

Кроме аналогичных требований, предъявляемых ко второму уровню контроля, дополнительно предъявляются следующие требования:

контроль соответствия исходных текстов ПО его объектному (загрузочному) коду с использованием сертифицированных компиляторов;

семантический контроль наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных конструкций.

3.5.4. Динамический анализ исходных текстов программ

Требования полностью включают в себя аналогичные требования ко второму уровню контроля.

3.5.5. Отчетность

Кроме аналогичных требований, предъявляемых ко второму уровню контроля, дополнительно отчет (протокол) должен содержать результаты:

контроля соответствия исходных текстов ПО его объектному (загрузочному) коду с использованием сертифицированных компиляторов;

семантического контроля наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных конструкций.