13

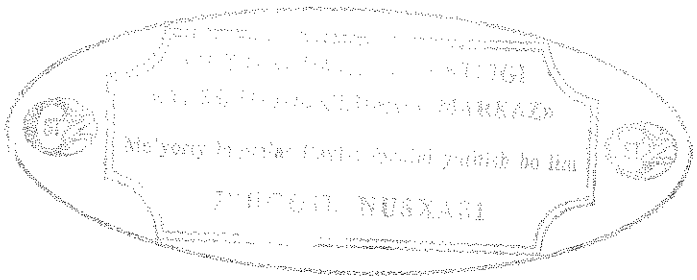
O‘z DSt 2116:2014

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недекларированных возможностей

Издание официальное



Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

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 № 05-930

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»

STANDARTLASHTIRISH, M
NAZORATINI MUVOFIQLASHTI
AXBOROT TEXNOLOGIYA
JORIY ETISH BO

Содержание

1 Область применения.....1
2 Нормативные ссылки.....1
3 Термины и определения.....2
4 Общие положения.....3
5 Требования к третьему уровню контроля.....5
6 Требования ко второму уровню контроля.....6
7 Требования к первому уровню контроля.....7

O‘zstandart agentligi
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BO‘LIMI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси
Ахборотни муҳофаза қилиш воситаларининг дастурий таъминотини декларация қилинмаган имкониятлар йўқлигини назорат қилиш даражаси бўйича таснифлаш

Информационная технология
Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недекларированных возможностей

Information technology
Classification of software of information protection means by levels of control absence from not declared functions

Дата введения 31.03.2014

1 Область применения

Настоящий стандарт устанавливает классификацию программного обеспечения (как отечественного, так и импортного производства) средств защиты информации, предназначенного для защиты информации ограниченного доступа, в том числе и встроенных в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недекларированных возможностей.

Стандарт предназначен для специалистов испытательных лабораторий, заказчиков, разработчиков программного обеспечения средств защиты информации при его контроле в части отсутствия недекларированных возможностей.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ 19.202-78 Единая система программной документации. Спецификация. Требования к содержанию и оформлению

ГОСТ 19.401-2000 Единая система программной документации. Текст программы. Требования к содержанию, оформлению и контролю качества

O'ZSTANDART AGENTLIGI
9200 son olingan
«18» 03 2014 yilda
Davlat ro'yxatiga olindi

ГОСТ 19.402-2000 Единая система программной документации. Описание программы. Требования к содержанию, оформлению и контролю качества

ГОСТ 19.404-79 Единая система программной документации. Пояснительная записка. Требования к содержанию и оформлению

ГОСТ 19.502-78 Единая система программной документации. Описание применения. Требования к содержанию и оформлению

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **динамический анализ исходных текстов программ:** Совокупность методов контроля соответствия/несоответствия реализованных и декларированных в документации функциональных возможностей программного обеспечения, основанных на идентификации фактических маршрутов выполнения функциональных объектов с последующим сопоставлением маршрутам, построенным в процессе проведения статического анализа.

3.2 **информационный объект**: Элемент программы (переменные, массивы, записи, таблицы, файлы, фрагменты оперативной памяти и т.п.), содержащий фрагменты информации, циркулирующей в программе.

3.3 **критический маршрут выполнения функциональных объектов:** Маршрут, при выполнении которого существует возможность неконтролируемого нарушения установленных правил обработки информационных объектов.

3.4 **маршрут выполнения функциональных объектов:** Определенная алгоритмом последовательность выполняемых функциональных объектов.

3.5 **недекларированные возможности**: Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

3.6 **программное обеспечение;** ПО: Совокупность системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

3.7 **программные закладки**: Преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.

3.8 **средства защиты информации**; СЗИ: Технические, криптографические, программные и другие средства, предназначенные для

O'ZBEKISTON RESPUBLIKASI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARI
MARKAZI ETIGI BILAN NUSXALANDI

защиты информации, средств, в которых они реализованы, а также средства контроля эффективности защиты информации.

3.9 **статический анализ исходных текстов программ:** Совокупность методов контроля соответствия/несоответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на структурном анализе и декомпозиции исходных текстов программ.

3.10 **фактический маршрут выполнения функциональных объектов:** Последовательность фактически выполняемых функциональных объектов при определённых условиях (входных данных).

3.11 **функциональный объект**: Элемент программы (процедуры, функции, ветви, операторы и т.п.), осуществляющий выполнение действий по реализации законченного фрагмента алгоритма программы.

4 Общие положения

4.1 Реализацией недекларированных возможностей, в частности, являются программные закладки.

4.2 Уровень контроля отсутствия недекларированных возможностей определяется выполнением заданного настоящим стандартом набора требований, предъявляемого к:

- составу и содержанию документации, представляемой заявителем для проведения испытаний ПО СЗИ;
- содержанию испытаний.

4.3 Устанавливается три уровня контроля отсутствия недекларированных возможностей. Каждый уровень характеризуется определенной минимальной совокупностью требований, приведенной в таблице 1.

Таблица 1

Наименование требования	Уровень контроля		
	3	2	1
Требования к документации			
1 Контроль состава и содержания документации			
1.1 Спецификация (ГОСТ 19.202)	+	+	+
1.2 Описание программы (ГОСТ 19.402)	+	+	+
1.3 Описание применения (ГОСТ 19.502)	+	+	+
1.4 Пояснительная записка (ГОСТ 19.404)	-	+	+
1.5 Тексты программ, входящих в состав ПО (ГОСТ 19.401)	+	+	+

O'ZBEKISTON RESPUBLIKASI STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARI AGENTLIGI

Окончание таблицы 1

Наименование требования	Уровень контроля		
	3	2	1
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 маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа	-	+	+
5 Отчетность	+	+	+
Примечание - «+» - есть требования к данному классу, «-» - нет требований к данному классу.			

Самый высокий уровень контроля - первый, определяется для ПО, используемого при защите информации с грифом «Совершенно секретно» (СС) и выше.

Второй уровень контроля достаточен для ПО, используемого при защите информации с грифом «Секретно» (С).

Самый низкий уровень контроля - третий, достаточен для ПО, используемого при защите конфиденциальной информации.

O'zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH
AXBOROT TEXNOLOGIYALARI
JORIY ETISH BO'LIMIDAGI

5 Требования к третьему уровню контроля

5.1. Контроль состава и содержания документации

В состав документации, представляемой заявителем на сертификационные испытания, должны входить:

- спецификация, составленная по ГОСТ 19.202 и содержащая сведения о составе ПО и документации на него;
- описание программы, соответствующее требованиям ГОСТ 19.402 и 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 по ГОСТ 19.502, 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, входящие в состав ПО, по ГОСТ 19.401.

Для ПО импортного производства состав документации может отличаться от требуемого, однако содержание должно соответствовать требованиям, указанным в вышеприведенных стандартах.

5.2 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.

5.3 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.

...STANDARTLASHTIRISH, DAVLAT ...NAZORATI VA MUVOFIQLASHTIRISH VA ...MOT TEXNOLOGIYALARIGA ...

5.4 Отчетность

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

- исходного состояния ПО;
- полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне файлов;
- соответствия исходных текстов ПО его объектному (загрузочному) коду.

6 Требования ко второму уровню контроля

6.1 Контроль состава и содержания документации

Требования аналогичны требованиям третьего уровня контроля, приведенным в 5.1.

Дополнительно должна быть представлена Пояснительная записка оформленная в соответствии с ГОСТ 19.404 и 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.

6.2 Контроль исходного состояния ПО

Требования аналогичны требованиям третьего уровня контроля, приведенным в 5.2.

6.3 Статический анализ исходных текстов программ

Требования аналогичны требованиям третьего уровня контроля, приведенным в 5.3.

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).

O‘zbekiston Agentligi
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARI
JORIY ETISH BOSHQARMASI

6.4 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.

6.5 Отчетность

Требования аналогичны требованиям третьего уровня контроля, приведенным в 5.4.

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.

7 Требования к первому уровню контроля

7.1 Контроль состава и содержания документации

Требования аналогичны требованиям второго уровня контроля, приведенным в 6.1.

7.2 Контроль исходного состояния ПО

Требования аналогичны требованиям второго уровня контроля, приведенным в 6.2.

7.3 Статический анализ исходных текстов программ

Требования аналогичны требованиям второго уровня контроля, приведенным в 6.3.

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.

7.4 Динамический анализ исходных текстов программ

Требования аналогичны требованиям второго уровня контроля, приведенным в 6.4.

Дополнительно предъявляются следующие требования:

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

7.5 Отчетность

Требования аналогичны требованиям второго уровня контроля, приведенным в 6.5.

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);

O'ZBEKISTON STANDARTLASHTIRISH MAZONATINI MUVOFIQLASHTIRISH AXBOROT TEXNOLOGIYALARI JORIY ETILISHI MUQOBILLIGI

- 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.

...ASI AGENTLIYI
...LAŞTIRILMA DAVLAT
...STANDARTLAŞDIRILMA VƏ
...MƏHSULLARININ
...ŞURULMASI

УДК 004.056.53 ОКС 35.040 П 89

Ключевые слова: программное обеспечение, недекларированные возможности, статистический анализ, динамический анализ, исходный текст, документация

MUVOFIQLASHTIRISH AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH
AXBOROT TEXNOLOGIYALARI
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

...STANDART AGENTLIGI
ST...NDARTLASHTIRISH, DAVLAT
...ZI...T AXBOROTLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI