ЕВРАЗИЙСКИЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ
И СЕРТИФИКАЦИИ (ЕАСС)

EURO-ASIAN COUNCIL FOR STANDARDIZATION, METROLOGY
AND CERTIFICATION (EASC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 31078–2002

Защита информации

ИСПЫТАНИЯ ПРОГРАММНЫХ СРЕДСТВ НА НАЛИЧИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ

Типовое руководство

Издание официальное

Зарегистрирован

№ 4369

" 4 " марта 2003 г.

Минск
Евразийский совет по стандартизации, метрологи и сертификации
2003

Предисловие

Евразийский Совет по стандартизации, метрологии и сертификации (ЕАСС) представляет собой региональное объединение национальных органов по стандартизации государств, входящих в содружество Независимых Государств. В дальнейшем возможно вступление в ЕАСС национальных органов по стандартизации других государств.

Цели, основные принципы и основной порядок проведения работ по межгосударственной стандартизации установлены ГОСТ 1.0-92 "Межгосударственная система стандартизации. Основные положения" и ГОСТ 1.2-97 "Межгосударственная система стандартизации. Стандарты межгосударственные, правила, рекомендации по межгосударственной стандартизации. Порядок разработки, принятия, обновления и отмены".

Сведения о стандарте

1 РАЗРАБОТАН 27 Центральным научно-исследовательским институтом Министерства обороны Российской Федерации (27 ЦНИИ МО РФ) и Научно-консультационным центром по созданию и применению информационных технологий (НКЦ «ЦНИИКА-СПИН»)

ВНЕСЕН Госстандартом России

2 ПРИНЯТ Евразийским Советом по стандартизации, метрологии и сертификации (протокол № 22 от 6 ноября 2002 г.)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004-97	Код страны по МК (ИСО 3166) 004-97	Сокращенное наименование национального органа по стандартизации
Армения	AM	Армгосстандарт
Беларусь	BY	Госстандарт Республики Беларусь
Казахстан	KZ	Госстандарт Республики Казахстан
Кыргызстан	KG	Кыргызстандарт
Молдова	MD	Молдовастандарт
Российская Федерация	RU	Госстандарт России

3 Настоящий стандарт идентичен ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»

4 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных (государственных) стандартов, издаваемых в этих государствах.

Информация об изменениях к настоящему стандарту публикуется в указателе (каталоге) "Межгосударственные стандарты", а текст изменений – в информационных указателях "Межгосударственные стандарты". В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе "Межгосударственные стандарты".

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

Защита информации

ИСПЫТАНИЯ ПРОГРАММНЫХ СРЕДСТВ НА НАЛИЧИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ

Типовое руководство

Information security. Software testing for the existence of computer viruses. The sample manual

Дата принятия 2002-11-06

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящий стандарт распространяется на испытания программных средств (ПС) и их компонентов, цели которых — обнаружить в этих ПС и устранить из них компьютерные вирусы (КВ) силами специальных предприятий (подразделений), и устанавливает общие требования к организации и проведению таких испытаний.

1.2 Требования, установленные настоящим стандартом, направлены на обеспечение специальной обработки ПС в целях выявления КВ, а также на устранение последствий, вызванных возможными воздействиями КВ на операционные системы, системные и пользовательские файлы с программами и данными, начальные секторы магнитных дисков, таблицы размещения файлов и др.

1.3 Настоящий стандарт устанавливает типовые требования, предъявляемые к испытаниям ПС на наличие КВ, в том числе:

- к составу мероприятий по подготовке и проведению испытаний;
- к составу, структуре и назначению основных частей программно-аппаратного стенда, обеспечивающего проведение испытаний;
- к выбору и использованию методов проведения испытаний;
- к тестовым (антивирусным) программам, обнаруживающим и уничтожающим КВ;
- к составу и содержанию документации, фиксирующей порядок проведения испытаний и их результаты.

1.4 Настоящий стандарт предназначен для применения в испытательных лабораториях, проводящих сертификационные испытания ПС на выполнение требований защиты информации.

2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящем стандарте использована ссылка на следующий стандарт:

ГОСТ 19.301—79 ЕСПД. Программа и методика испытаний. Требования к содержанию и оформлению

3 ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящем стандарте применены следующие термины с соответствующими определениями:

Защита программных средств — организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий.

Сертификация — действия третьей стороны, цель которых — подтвердить (с помощью сертификата соответствия) то, что изделие (в том числе программное средство) или услуга соответствует определенным стандартам или другим нормативным документам.

Профилактика — систематические действия эксплуатационного персонала, цель которых — выявить и устранить неблагоприятные изменения в свойствах и характеристиках используемых программных средств, в частности проверить эксплуатируемые, хранимые и (или) вновь полученные программные средства на наличие компьютерных вирусов.

Издание официальное

★

Ревизия — проверка вновь полученных программ специальными средствами, проводимая путем их запуска в контролируемой среде.

Несанкционированный доступ к программным средствам — доступ к программам, записанным в памяти ЭВМ или на машинном носителе, а также отраженным в документации на эти программы, осуществленный с нарушением установленных правил.

Вакцинирование — обработка файлов, дисков, каталогов, проводимая с применением специальных программ, создающих условия, подобные тем, которые создаются определенным компьютерным вирусом, и затрудняющих повторное его появление.

Компьютерный вирус — программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

В настоящем стандарте приняты следующие сокращения:

- ПС — программные средства.
- КВ — компьютерные вирусы.
- ПЭВМ — персональная электронно-вычислительная машина (персональный компьютер).
- ЭВМ — электронно-вычислительная машина.

4 ПОРЯДОК ПРОВЕДЕНИЯ ИСПЫТАНИЙ ПРОГРАММНЫХ СРЕДСТВ НА НАЛИЧИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ

4.1 Испытания ПС на наличие КВ следует проводить на специально оборудованном программно-аппаратном испытательном стенде, в составе которого должны быть необходимые технические и программные средства, в том числе антивирусные программы.

4.2 Предприятие [подразделение (далее — организация)], проводящее проверку ПС на наличие КВ, должно поддерживать испытательный стенд в работоспособном состоянии и не допускать проникновения КВ в программы и данные до начала проведения испытаний.

4.3 Организация, проводящая проверку ПС на наличие КВ, должна определить и зафиксировать в программе испытаний цель и объем испытаний, а также свои обязательства, касающиеся мер защиты проверяемых ПС от их заражения КВ с учетом требований ГОСТ 19.301.

4.4 Меры по защите проверяемых ПС от заражения КВ могут включать в себя:

- разработку и выполнение комплекса мероприятий по профилактике, ревизии и вакцинированию используемых ПС;
- подготовку должностных лиц, отвечающих за проведение испытаний ПС;
- разработку и выбор способов применения программно-технических средств для обнаружения КВ в ПС;
- взаимодействие организаций, заказывающих и проводящих испытания ПС;
- контроль за проведением испытаний ПС;
- оценку эффективности применяемых антивирусных средств;
- совершенствование системы мероприятий по защите ПС от КВ на основе современных достижений информационной технологии;
- установление административной ответственности должностных лиц за выполнение требований защиты ПС от КВ;
- назначение ответственных должностных лиц и определение их полномочий, относящихся к организации и проведению мероприятий по защите ПС от КВ.

4.5 Организация, выполняющая проверку ПС на наличие КВ, должна обеспечить весь процесс проверки необходимыми вычислительными техническими и программными средствами, а также назначить специально обученных сотрудников для проведения испытаний.

4.6 Организация, выполняющая проверку ПС на наличие КВ, должна назначить постоянного представителя, который получает определенные полномочия и несет постоянную ответственность за выполнение требований, установленных настоящим стандартом.

4.7 В состав технических средств испытательного стенда должны входить:

- совместимые ПЭВМ;
- необходимые элементы телекоммуникационных сетей;
- каналы связи.

4.8 Конкретный набор технических компонентов испытательного стенда должен быть таким, чтобы были обеспечены условия воспроизведения всех необходимых внешних воздействий на ПС в процессе проведения испытаний.