ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57429— 2017

СУДЕБНАЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА

Термины и определения

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным бюджетным учреждением «Российский федеральный центр судебной экспертизы» при Министерстве юстиции Российской Федерации совместно с Федеральным государственным казенным учреждением «Экспертно-криминалистический центр Министерства внутренних дел Российской Федерации», ФГБОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)», Следственным комитетом Российской Федерации

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 134 «Судебная экспертиза»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2017 г. № 198-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Август 2018 г.

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Термины и определения 1
Алфавитный указатель терминов на русском языке 5
Алфавитный указатель терминов на английском языке 6

Введение

Установленные в настоящем стандарте термины расположены в систематизированном порядке, отражающем систему понятий судебной компьютерно-технической экспертизы.

Для каждого понятия установлен один стандартизованный термин.

Термины-синонимы приведены в качестве справочных данных и не являются стандартизованными.

Приведенные определения можно при необходимости изменять, вводя в них производные признаки, раскрывая значения используемых в них терминов, указывая объекты, входящие в объем определяемого понятия. Изменения не должны нарушать объем и содержание понятий, определенных в настоящем стандарте.

В стандарте приведены иноязычные эквиваленты стандартизованных терминов на английском языке.

Стандартизованные термины набраны полужирным шрифтом, их краткие формы, представленные аббревиатурой, — светлым, синонимы — курсивом.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СУДЕБНАЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА

Термины и определения

Forensic information technology examination. Terms and definitions

Дата введения — 2017—09—01

1 Область применения

Настоящий стандарт устанавливает термины и определения понятий, применяемые в судебной компьютерно-технической экспертизе.

Термины, устанавливаемые настоящим стандартом, рекомендуются для применения во всех видах документации и литературы в области судебной компьютерно-технической экспертизы, входящих в сферу действия работ по стандартизации и (или) использующих результаты этих работ. Требования стандарта распространяются как на государственных судебных экспертов, так и на негосударственных судебных экспертов.

2 Термины и определения

Общие понятия

1 **антивирусное программное обеспечение:** Специализированное программное обеспечение для обнаружения нежелательных программ, восстановления измененных такими программами файлов, а также для предотвращения изменения такими программами файлов или операционной системы.	anti-virus software
1.1 **компьютерный вирус:** Программа, обладающая способностью к самораспространению по локальным ресурсам средства вычислительной техники, не использующая сетевых сервисов.	computer virus, virus
1.2 **троянская программа:** Программа, не обладающая возможностью самораспространения, маскирующаяся под легитимный файл.	trojan
1.3 **червь:** Программа, обладающая способностью к самораспространению в компьютерных сетях через сетевые ресурсы.	worm
2 **аппаратное средство** *(техническое средство)*: Совокупность технических устройств средств вычислительной техники либо их частей.	hardware
3 **базовая система ввода/вывода:** Набор программ управления основными функциями и устройствами средства вычислительной техники.	basic input/output system; BIOS
4 **вычислительная сеть:** Совокупность средств вычислительной техники, соединенных между собой, обеспечивающих передачу данных посредством телекоммуникационной связи.	computer network
5 **средство вычислительной техники;** СВТ: Совокупность технических устройств и программ, обеспечивающих их функционирование, способных функционировать самостоятельно или в составе других систем.	computer
6 **интерфейс:** Совокупность возможностей одновременного совместного действия двух линейно не связанных систем либо системы и человека.	interface

Издание официальное

7 **кластер:** Объединение нескольких однородных элементов, которое может рассматриваться как самостоятельная единица, обладающая определенными свойствами.	cluster
8 **оперативная память** (*основная память*): Память, предназначенная для временного хранения данных и команд.	main memory, randomaccess memory; RAM
9 **операционная система;** ОС: Комплекс взаимосвязанных программ, предназначенных для управления ресурсами средств вычислительной техники и организации взаимодействия с пользователем.	operating system; OS
10 **прошивка:** Программа, записанная на микросхеме постоянного запоминающего устройства и управляющая работой аппаратного средства.	firmware
11 **электронная почта:** Корреспонденция в виде сообщений, передаваемая между пользователями через вычислительную сеть.	e-mail

Понятия, относящиеся к исследованию информации

12 **авторизация:** Предоставление определенному лицу или группе лиц прав на выполнение определенных действий, а также процесс подтверждения данных прав при попытке выполнения этих действий.	authorization
13 **адрес:** Уникальный в пределах конкретного пространства код, присваиваемый устройству, объекту для операций с ним.	address
14 **активация:** Приведение объекта в состояние готовности к действию или использованию.	activation
15 **алгоритм:** Конечное упорядоченное множество точно определенных правил для решения конкретной задачи. ГОСТ Р 52292—2004, ст. 7.1.2.	algorithm
16 **архивирование:** Преобразование данных в компактную форму без потери содержащейся в них информации с помощью специализированной программы с целью экономии места на носителе информации и/или повышения эффективности передачи данных.	archiving
17 **архивный файл:** Файл, полученный в результате архивирования одного или нескольких файлов.	archived file
18 **разархивирование:** Извлечение файлов из архивного файла.	unpack
19 **атрибуты файла:** Характеристики файла, определяемые операционной системой и прикладным программным обеспечением.	file attributes
20 **аутентификация пользователя:** Процедура проверки подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных пользователей.	user authentification
21 **аутентификация электронного письма:** Подтверждение подлинности электронного письма путем проверки цифровой подписи письма по открытому ключу отправителя.	e-mail authentification
22 **аутентификация файла:** Проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.	file authentification
23 **база данных;** БД: Совокупность взаимосвязанных данных, организованных в соответствии со структурой и правилами обеспечения целостности данных таким образом, чтобы с ними мог работать пользователь.	database; DB
24 **межсетевой экран** (*брендмауэр; файерволл*): Комплекс аппаратных и/или программных средств в вычислительной сети, осуществляющий контроль и фильтрацию проходящей через него информации в соответствии с заданными правилами. Примечание — Основной задачей сетевого экрана является защита сети или отдельных ее узлов от воздействия со стороны внешних вычислительных сетей.	firewall
25 **браузер** (*броузер*): Программа для поиска и просмотра информации из вычислительной сети.	browser

26 **виртуальная машина:** Программная среда, которая внутри одной программной и/или аппаратной системы эмулирует работу другой программной и/или аппаратной системы.	virtual machine
27 **восстановление поврежденного файла:** Процесс восстановления структуры файла с целью получения доступа к информации.	file recovery
28 **восстановление удаленного файла:** Процесс получения доступа к информации, размещенной на машинном носителе в областях, ранее определенных файловой системой как конкретный файл.	file undelete
29 **временный файл:** Файл, создаваемый программой на ограниченное время.	temporary file, tempfile
30 **дистрибутив:** Форма распространения программного обеспечения. Примечание — Как правило, содержит набор файлов, составляющих программу, инструкции по установке, зависимости от других программ и автоматизированный установщик.	distributive
31 **динамический анализ программного кода:** Определение функциональных возможностей программного обеспечения экспериментальным путем.	dynamic program analysis
32 **имя пользователя:** Имя учетной записи пользователя, которое может представлять собой как подлинные фамилию и имя или инициалы пользователя, так и псевдоним.	user name
33 **инсталляция:** Установка программного обеспечения в вычислительной системе с дистрибутива.	installation, setup
34 **исполняемый файл:** Файл, содержащий готовую к исполнению программу.	executable file
35 **исходный код** (*исходный текст*): Текст программы на каком-либо языке программирования или языке разметки.	source code
36 **каталог:** Список объектов файловой системы с указанием их месторасположения в разделе.	directory, folder
37 **меню:** Список параметров, из которого пользователь может выбрать параметр для выполнения требуемого действия.	menu
38 **метаданные файла:** Атрибуты файла, определяемые прикладным программным обеспечением.	metadata
39 **повреждение файла:** Нарушение структуры файла.	file damage
40 **структура файла:** Соглашение о внутреннем устройстве файла, в соответствии с которым размещается и интерпретируется его содержание.	file structure
41 **прикладная программа:** Программа, предназначенная для решения конкретных задач пользователя, использующая для управления ресурсами средств вычислительной техники операционную систему.	application program
42 **программа:** Последовательность инструкций, определяющих решение конкретной задачи вычислительной системой.	program
43 **протокол работы программы:** Файл с записями о событиях в хронологическом порядке.	journal, log
44 **раздел:** Часть машинного носителя либо кластера машинных носителей, логически выделенная для удобства работы.	partition
45 **куст реестра** *(ветвь реестра)*: Группа разделов, подразделов и параметров реестра с набором вспомогательных файлов, содержащих резервные копии этих данных.	hive
46 **раздел реестра** *(ключ реестра)*: Заголовок реестра, обеспечивающий структуру для хранения конфигурационных значений и другой информации, которая необходима ОС Windows и установленным в ней приложениям.	registry key
47 **свойства файла:** Атрибуты файла, определяемые операционной системой.	file properties
48 **сигнатура файла:** Уникальная цепочка байт или формализованное описание признаков, указывающие на тип файла.	file signature

49 **системный реестр:** Иерархически построенная база данных для хранения сведений, необходимых для настройки операционной системы, для работы с пользователями, программными продуктами и устройствами, в большинстве операционных систем ОС Windows.	Windows Registry
50 **статический анализ программного кода:** Определение функциональных возможностей программного обеспечения путем изучения составных частей, элементов исходного или машинного кода.	static code analysis
51 **удаление файла:** Изменение состояния объекта с использованием стандартных средств операционной системы, при котором его дальнейшее использование становится невозможным.	file delete
52 **удаленный доступ:** Процесс получения доступа к средствам вычислительной техники посредством вычислительной сети с использованием другого средства вычислительной техники.	remote access
53 **учетная запись:** Совокупность данных о пользователе, необходимая для его аутентификации и предоставления доступа к его личным данным и настройкам.	account
54 **файл:** Поименованный набор данных, расположенный на машинном носителе информации.	file
55 **файловая система:** Описание способа хранения, распределения, наименования и обеспечения доступа к информации, хранящейся на машинном носителе информации. Примечание — Определяет правила наименования файлов и каталогов, ограничения на максимальные размеры файла и раздела, длину имени файла, максимальный уровень вложенности каталогов и др.	file system
56 **хеш-функция:** Функция, выполняющая по определенному алгоритму преобразование входящих данных сколь угодно большого размера в битовую строку фиксированной длины.	hash function
57 **хеш-код** *(хеш-значение)*: Битовая строка фиксированной длины, являющаяся результатом преобразования входящих данных хеш-функцией. Примечание — Для одного и того же объекта хеш-код всегда одинаков; для одинаковых объектов хеш-коды одинаковы; если хеш-коды равны, то входные объекты не всегда равны; если хеш-коды не равны, то и объекты не равны.	hash code
58 **эмуляция:** Имитация работы одной системы средствами другой без потери функциональных возможностей и искажений результатов.	emulation
59 **эмулятор:** Программа или микросхема, позволяющая осуществлять эмуляцию.	emulator
60 **ярлык:** Специальный вид файла, служащий указателем на объект, программу или команду и содержащий в себе полный путь до объекта, на который ссылается.	shortcut

Понятия, относящиеся к аппаратному исследованию

61 **адаптер:** Приспособление, устройство или деталь, предназначенные для соединения устройств, не имеющих совместимого способа соединения.	adapter
62 **драйвер устройства:** Программа, предоставляющая возможности для управления определенным типом устройства операционной системе и прикладным программам.	driver
63 **коммутатор:** Устройство, объединяющее различные сетевые устройства в единый сегмент сети и передающее информацию конкретному устройству.	switch
64 **концентратор:** Устройство, объединяющее различные сетевые устройства в единый сегмент сети и передающее информацию всем устройствам.	hub
65 **маршрутизатор:** Специализированный сетевой компьютер, имеющий два или более сетевых интерфейса и пересылающий пакеты данных между различными сегментами сети.	router

Алфавитный указатель терминов на русском языке

авторизация 12
адаптер 61
адрес 13
активация 14
алгоритм 15
анализ программного кода динамический 31
анализ программного кода статический 50
архивирование 16
атрибуты файла 19
аутентификация пользователя 20
аутентификация файла 22
аутентификация электронного письма 21
база данных 23
БД 23
браузер 25
брендмауэр 24
броузер 25
ветвь реестра 45
вирус компьютерный 1.1
восстановление поврежденного файла 27
восстановление удаленного файла 28
дистрибутив 30
доступ удаленный 52
драйвер устройства 62
запись учетная 53
имя пользователя 32
инсталляция 33
интерфейс 6
каталог 36
кластер 7
ключ реестра 46
код исходный 35
коммутатор 63
концентратор 64
куст реестра 45
маршрутизатор 65
машина виртуальная 26
меню 37
метаданные файла 38
обеспечение программное антивирусное 1
ОС 9
память оперативная 8
память основная 8
повреждение файла 39
почта электронная 11
программа 42
программа прикладная 41
программа троянская 1.2
протокол работы программы 43
прошивка 10
разархивирование 18
раздел 44
раздел реестра 46

реестр системный 49
свойства файла 47
СВТ 5
сеть вычислительная 4
сигнатура файла 48
система ввода/вывода базовая 3
система операционная 9
система файловая 55
средство аппаратное 2
средство технических 2
средство вычислительной техники 5
структура файла 40
текст исходный 35
удаление файла 51
файервол 24
файл 54
файл архивный 17
файл временный 29
файл исполняемый 34
хеш-значение 57
хеш-код 57
хеш-функция 56
червь 1.3
экран межсетевой 24
эмулятор 59
эмуляция 58
ярлык 60

Алфавитный указатель терминов на английском языке

account 53
activation 14
adapter 61
address 13
algorithm 15
anti-virus software 1
application program 41
archived file 17
archiving 16
authorization 12
basic input/output system 3
BIOS 3
browser 25
cluster 7
computer 5
computer network 4
computer virus 1.1
database 23
DB 23
directory 36
distributive 30
driver 62
dynamic program analysis 31

e-mail 11
e-mail authentification 21
emulation 58
emulator 59
executable file 34
file 54
file attributes 19
file authentification 22
file damage 39
file delete 51
file properties 47
file recovery 27
file signature 48
file structure 40
file system 55
file undelete 28
firewall 24
firmware 10
folder 36
hardware 2
hash code 57
hash function 56
hive 45
hub 64
installation 33
interface 6
journal 43
log 43
main memory 8
menu 37
metadata 38
operating system 9
OS 9
partition 44
program 42
RAM 8
random-access memory 8
registry key 46
remote access 52
router 65
setup 33
shortcut 60
source code 35
static code analysis 50
switch 63
tempfile 29
temporary file 29
trojan 1.2
unpack 18
user authentification 20
user name 32
virtual machine 26
virus 1.1
Windows Registry 49
worm 1.3

УДК 006.72:006.354 ОКС 01.040.01

Ключевые слова: компьютерно-техническая экспертиза, компьютерная экспертиза, информационное исследование, аппаратное исследование

Редактор *Е.В. Лукьянова*
Технический редактор *И.Е. Черепкова*
Корректор *М.В. Бучная*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 30.07.2018. Подписано в печать 09.08.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,26.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 123001 Москва, Гранатный пер., 4.
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru