ГОСТ Р 57429-2017

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СУДЕБНАЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА

Термины и определения

Forensic information technology examination. Terms and definitions

ОКС 01.040.01

Дата введения 2017-09-01

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. N 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. N 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 (www.gost.ru)*

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.

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
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, random access memory; RAM
9 **операционная система;** ОС: Комплекс взаимосвязанных программ, предназначенных для управления ресурсами средств вычислительной техники и организации взаимодействия с пользователем.	operating system; OS
1 0 **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

1 2 **авторизация:** Предоставление определенному лицу или группе лиц прав на выполнение определенных действий, а также процесс подтверждения данных прав при попытке выполнения этих действий. authorization

1 3 **адрес:** Уникальный в пределах конкретного пространства код, присваиваемый устройству, объекту для операций с ним. address

1 4 **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

1 6 **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

1 8 **разархивирование:** Извлечение файлов из архивного файла. unpack

1 9 **атрибуты файла:** Характеристики файла, определяемые операционной системой и прикладным программным обеспечением. file attributes

2 0 **аутентификация пользователя:** Процедура проверки подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных пользователей. user authentification

2 1 **аутентификация электронного письма:** Подтверждение подлинности электронного письма путем проверки цифровой подписи письма по открытому ключу отправителя. e-mail authentification

2 2 **аутентификация файла:** Проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла. file authentification

2 3 **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

2 4 **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. firewall

Примечание - Основной задачей сетевого экрана является защита сети или отдельных ее узлов от воздействия со стороны внешних вычислительных сетей.

2 5 **браузер** (*броузер*): Программа для поиска и просмотра информации из вычислительной сети. browser

2 6 **виртуальная машина:** Программная среда, которая внутри одной программной и/или аппаратной системы эмулирует работу другой программной и/или аппаратной системы. virtual machine

2 7 **восстановление поврежденного файла:** Процесс восстановления структуры файла с целью получения доступа к информации. file recovery

2 8 **восстановление удаленного файла:** Процесс получения доступа к информации, размещенной на машинном носителе в областях, ранее определенных файловой системой как конкретный файл. file undelete

2 9 **временный файл:** Файл, создаваемый программой на ограниченное время. temporary file, tempfile

3 0 **дистрибутив:** Форма распространения программного обеспечения.

Примечание - Как правило, содержит набор файлов, составляющих программу, инструкции по установке, зависимости от других программ и автоматизированный установщик. distributive

3 1 **динамический анализ программного кода:** Определение функциональных возможностей программного обеспечения экспериментальным путем. dynamic program analysis

3 2 **имя пользователя:** Имя учетной записи пользователя, которое может представлять собой как подлинные фамилию и имя или инициалы пользователя, так и псевдоним. user name

3 3 **инсталляция:** Установка программного обеспечения в вычислительной системе с дистрибутива. installation, setup

34 **исполняемый файл:** Файл, содержащий готовую к исполнению программу. executable file

3 5 **исходный код** (*исходный текст*): Текст программы на каком-либо языке программирования или языке разметки. source code

3 6 **каталог:** Список объектов файловой системы с указанием их месторасположения в разделе. directory, folder

3 7 **меню:** Список параметров, из которого пользователь может выбрать параметр для выполнения требуемого действия. menu

3 8 **метаданные файла:** Атрибуты файла, определяемые прикладным программным обеспечением. metadata

3 9 **повреждение файла:** Нарушение структуры файла. file damage

4 0 **структура файла:** Соглашение о внутреннем устройстве файла, в соответствии с которым размещается и интерпретируется его содержание. file structure

4 1 **прикладная программа:** Программа, предназначенная для решения конкретных задач пользователя, использующая для управления ресурсами средств вычислительной техники операционную систему. application program

4 2 **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

4 6 **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

4 7 **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

4 9 **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

5 0 **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

5 3 **учетная запись:** Совокупность данных о пользователе, необходимая для его аутентификации и предоставления доступа к его личным данным и настройкам. account

5 4 **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. file system

Примечание - Определяет правила наименования файлов и каталогов, ограничения на максимальные размеры файла и раздела, длину имени файла, максимальный уровень вложенности каталогов и др.

5 6 **хеш-функция:** Функция, выполняющая по определенному алгоритму преобразование входящих данных сколь угодно большого размера в битовую строку фиксированной длины. hash function

5 7 **хеш-код** (*хеш-значение*): Битовая строка фиксированной длины, являющаяся результатом преобразования входящих данных хеш-функцией. hash code

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.

5 8 **эмуляция:** Имитация работы одной системы средствами другой без потери функциональных возможностей и искажений результатов. emulation

5 9 **эмулятор:** Программа или микросхема, позволяющая осуществлять эмуляцию. emulator

6 0 **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

6 1 **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

6 4 **концентратор:** Устройство, объединяющее различные сетевые устройства в единый сегмент сети и передающее информацию всем устройствам. hub

6 5 **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

Алфавитный указатель терминов на английском языке

УДК 006.72:006.354 ОКС 01.040.01

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

Электронный текст документа
подготовлен АО "Кодекс" и сверен по:
официальное издание
М.: Стандартинформ, 2018