Министерство внутренних дел Российской Федерации
Омская академия

А. И. Горев, А. А. Симаков

ОБРАБОТКА И ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Учебно-практическое пособие

Омск
ОмА МВД России
2016

УДК 654 (075.8)
ББК 32.97
Г 69

Рецензенты:
кандидат физико-математических наук, доцент *С. В. Мухачёв*
(Уральский юридический институт МВД России);
кандидат технических наук, доцент *А. Н. Прокопенко*
(Белгородский юридический институт МВД России имени И. Д. Путилина)

Горев, А. И.

Г 69 Обработка и защита информации в компьютерных системах : учеб.-практ. пособие / А. И. Горев, А. А. Симаков. — Омск : Омская академия МВД России, 2016. — 88 с.

ISBN 978-5-88651-642-5

Повсеместное применение современных информационных технологий в процессе хранения, обработки и передачи информации накладывает определенные требования к компетентности сотрудника органов внутренних дел как пользователя информационных ресурсов и систем. Для качественного выполнения служебных обязанностей сотрудникам необходимы практические навыки быстрого поиска востребованных данных из большого объема общедоступной информации в локальных ресурсах и сети Интернет, восстановления поврежденной или удаленной информации с персонального компьютера, ее защиты стандартными и доступными программными средствами обработки и анализа полученной информации.

Пособие предназначено для курсантов и слушателей образовательных организаций МВД России, сотрудников криминальной полиции и следственных подразделений органов внутренних дел.

УДК 654 (075.8)
ББК 32.97

ISBN 978-5-88651-642-5

ВВЕДЕНИЕ

Современное общество — общество информационное. Информация стала в нем ресурсом более значимым, чем природные, трудовые и иные виды ресурсов. Она накапливается и собирается, продается и покупается, обменивается и распространяется. Однако внедрение современных компьютерных технологий обработки информации проходит бессистемно. Именно это и является причиной множественных ошибок и конфликтов в данной сфере.

Особую значимость компьютерные технологии обработки информации приобрели в последнее десятилетие, этот процесс затронул все сферы жизни общества. Прогрессивное развитие современного социума неразрывно связано с повышением роли процессов информатизации, которые выражаются в широком распространении разнообразных носителей информации в компьютерном формате хранения и в лавинообразном накоплении информации в базах данных операторов сетей.

При высоком уровне латентности количество выявленных преступлений в информационной сфере стремительно увеличивается, что требует адекватной реакции правоохранительных органов. Кроме того, компьютерные технологии все чаще используются при совершении традиционных видов преступлений и практически всегда — в сфере экономической деятельности.

ГЛАВА I. СТРУКТУРА ЗАПИСИ ИНФОРМАЦИИ НА НОСИТЕЛЬ

§ 1. Устройство магнитного диска

Существует много носителей для хранения компьютерной информации: магнитные, магнитооптические и оптические диски, флешнакопители. Конкретное устройство для сохранения информации может функционировать на основе специфичного физического явления, но для операционной системы оно предоставляет одинаковый механизм доступа к данным. Исключение составляют магнитные ленты, которые в настоящее время на практике не используются. Рассмотрим сохранение информации в файловой системе FAT на примере одного из самых распространенных носителей — магнитного диска. Принципы, по которым построена внутренняя организация магнитных дисков, не зависят от его вида (гибкий, фиксированный) и емкости.

В основе внутренней организации диска находится физическая структура, на уровне которой выделяются рабочие стороны: дорожки — ряды концентрических колец на поверхности одной стороны диска; секторы, радиально делящие дорожки. Для обращения к физическому сектору необходимо указывать номер стороны, номер дорожки и номер сектора на дорожке. Операционная система MS-DOS рассматривает все секторы диска как одну цепь с нумерацией, идущей подряд от нуля. Поэтому каждый сектор диска имеет свой логический номер.

На логическом уровне магнитный диск разделен на четыре области:

— загрузочный сектор (BOOT-сектор);

— таблица размещения файлов (FAT-таблица);

— корневой каталог (ROOT-каталог);

— область данных.

Фиксированные диски имеют и пятую область — таблицу разделов.

Заполнение диска осуществляется от наружной дорожки к центру. При периодическом удалении отдельных файлов секторы, занимаемые ими, освобождаются, при этом в различных частях диска появляются

свободные области. В результате информация, записываемая во вновь создаваемые файлы, может располагаться фрагментированно в секторах, которые были свободны в момент сохранения данной информации.

Операционная система хранит информацию в специальных логических образованиях — файлах. Каждому файлу однозначно соответствуют определенные секторы на диске. Данные о том, в каких секторах располагается информация конкретного файла, записывается в таблице размещения файлов (FAT), где объединение нескольких секторов (в качестве адресуемого элемента) называется кластером. В FAT-таблице позиция, соответствующая кластеру, с которого была начата запись информации файла, содержит ссылку на кластер, где хранится следующая часть информации из файла. Позиция, соответствующая второму кластеру, включает ссылку на третий и т. д.

Данные о том, с какого кластера начинается информация, сохраняемая в конкретном файле, запоминаются в специально отведенных зонах диска — каталогах. Физическая структура диска строго определяет местоположение только корневого каталога. Положение сведений, содержащихся во всех остальных каталогах, задается аналогично файлам: путем указания начальной позиции в ранее привязанных каталогах и соответствующей цепочки в FAT-таблице.

Существует строгая логическая система, которая определяет физические позиции диска, занятые информацией из конкретного файла:

1) загрузочный сектор диска, расположенный в первом секторе магнитного носителя, позволяет получить сведения о характеристиках (размер и местоположение) FAT-таблицы и корневого каталога;

2) корневой каталог, расположенный в фиксированном месте магнитного диска. Каждая запись в корневом каталоге соответствует некоторому файлу или каталогу, содержит номер первого кластера, занятого этим файлом (каталогом);

3) в ячейке FAT, соответствующей номеру первого кластера файла, содержится номер второго кластера. Далее в каждой очередной ячейке содержится номер следующего кластера. Ячейка, соответствующая последнему кластеру, содержит специальную пометку, обозначающую отсутствие продолжения.

Каждая из служебных областей магнитного диска выполняет определенную функцию по обслуживанию хранимой информации. При внесении изменений в указанные области может быть частично или полностью разрушен доступ к данным, что позволяет использовать эти приемы для сокрытия информации.

Загрузочный сектор (BOOT-сектор) содержит сведения о структуре диска. Операционная система при каждом обращении к диску проверяет BOOT-сектор для определения местоположения FAT и корневого каталога.

Если в BOOT-секторе записана неверная информация, то прочитать данные с диска средствами операционной системы нельзя. Попытки произвести чтение/запись с такого диска вызывают ошибочную ситуацию, что создает впечатление о бесполезности данного диска. В этом случае операционная система предлагает провести форматирование, что может привести к утрате информации.

Таблица размещения файлов FAT определяет, в каких секторах хранится информация из конкретного файла, а также в какой последовательности эти секторы считывать. Кроме того, в FAT содержатся и сведения о «сбойных» участках диска. Если во всех копиях FAT-таблицы записаны неверные данные, то файлы, ранее записанные на этом магнитном носителе, невозможно прочитать стандартными средствами операционной системы. При использовании такого приема доступ к файлу формально существует, но информация, получаемая обычным путем, в лучшем случае представляется совокупностью разрозненных фрагментов, а в худшем — лишенной смысла.

В секторах, отведенных под ***корневой каталог***, хранится информация об именах файлов и подкаталогов, об их размерах, датах создания или модификации, а также ссылки для FAT на начало файлов. Для хранения информации об одном файле выделяется 32 байта (табл. 1).

Таблица 1. **Структура записи в каталоге**

№ п/п	Занимаемые байты	Параметр
1	0–7	Имя файла (подкаталога)
2	8–10	Расширение файла
3	11	Атрибут файла
4	12–21	Зарезервировано
5	22–23	Время создания файла
6	24–25	Дата создания файла
7	26–27	Начальный кластер
8	28–31	Размер файла

Без данных, хранящихся в корневом каталоге, невозможно считать информацию с диска. Искажение ROOT-каталога может привести к ошибочному мнению о бесполезности диска.

Область данных магнитного диска используется для размещения информации, запоминаемой в виде файлов. В случае необходимости операционная система вычисляет (с помощью корневого каталога, каталогов и FAT-таблицы), с какими секторами диска работать при чтении/записи информации. Если информация в область данных заносится без соответствующих отметок в FAT-таблицах и каталогах, то операционная система считает, что данной информации на диске не существует. Этим свойством можно пользоваться для сокрытия сведений.

Удаление файла осуществляется путем изменения соответствующей записи в каталоге, содержащем удаляемый файл. Первый символ заменяется на специальный код E5h (в шестнадцатиричном представлении), остальная информация, хранящаяся в этой строке (размер файла, номер начального кластера и др.), остается без изменений до тех пор, пока в строке не будет записана информация о другом файле. Одновременно все ячейки FAT-таблицы, в которых хранилась информация о номерах кластеров, занятых этим файлом, объявляются свободными (заполняются кодом 00h) и могут быть использованы для сохранения новой информации. После указанных манипуляций операционная система более не располагает точными сведениями о местоположении всех кластеров, в которых хранилась информация из этого файла, что определяет вероятность некорректного восстановления информации из удаленных файлов.

Поскольку все обозначенные изменения не затрагивают непосредственно информацию, ранее хранившуюся в удаленном файле, то ее можно восстановить. Необходимая информация может быть успешно восстановлена при условии, что в кластеры диска, где она ранее содержалась, не были занесены новые данные.

Автоматические процедуры восстановления используют сведения о размере удаленного файла и номере начального кластера. На основе таких данных определяется местоположение файла на диске и количество принадлежащих этому файлу кластеров. В процессе автоматического восстановления осуществляется поиск соответствующего количества свободных кластеров начиная от кластера, указанного в каталоге в качестве первого. Все обнаруженные свободные кластеры признаются принадлежащими восстанавливаемому файлу. Поскольку между кластерами, ранее принадлежавшими удаленному файлу, могут оказаться свободные кластеры, ранее не принадлежавшие этому файлу, то чужие кластеры будут признаны принадлежащими данному файлу, а соответствующее количество необходимых кластеров не будет включено в восстановленный файл.

При определенной спорности подобного метода восстановления файлов, он позволяет пользователям, незнакомым с особенностями организации хранения информации на магнитных носителях, восстанавливать информацию из файлов, удаленных по неосторожности. Если удаленный файл занимал смежные кластеры магнитного диска, то автоматические процедуры восстановят его без ошибок. Единственная проблема, которую необходимо решить при восстановлении, — это указать некоторый символ в качестве первого символа названия файла. Вероятность корректного восстановления файла значительно повышается, если перед удалением файла выполнялась операция дефрагментации магнитного носителя, включающая перезапись информации из файлов в смежные кластеры диска (штатная программа операционной системы).

Процедуры восстановления файлов в ручном режиме дают возможность человеку определять принадлежность каждого конкретного кластера данному файлу, что делает процесс восстановления более гибким, но применимым только для текстовых файлов, информация которых может быть воспринята пользователем.

Сходными принципами определяется работа MS Windows. Удаляемые файлы только переносятся в так называемую корзину (Recycle Bin). Файл, находящийся в корзине, можно окончательно удалить либо восстановить (в зависимости от потребности).

Сокрытие важной информации путем удаления файлов и каталогов не может служить надежным способом укрытия данных от посторонних лиц. Наличие развитых средств восстановления ранее удаленных файлов и средств непосредственного поиска заданной информации в кластерах диска приводит с большой долей вероятности к выявлению таких файлов и считыванию из них информации.

Для гарантированного удаления конфиденциальной информации необходимо осуществить повторную запись произвольной информации в кластеры, ранее занимаемые удаленным файлом, либо произвести низкоуровневое (полное) форматирование диска. В режиме полного форматирования во всем пространстве диска записывается один и тот же специальный служебный символ, что полностью уничтожает всю ранее находившуюся на этом диске информацию. При форматировании в быстром режиме, т. е. без записи служебного символа, сохраняется возможность восстановления информации, утраченной в результате ошибочного форматирования или скрытой от посторонних глаз с применением этого механизма.

Потерянный кластер. В процессе эксплуатации на носитель влияет множество электромагнитных полей, в связи с чем возможны нарушения в работе различных элементов компьютера. В результате таких нарушений не исключены ситуации, когда часть пространства на магнитном носителе выпадает из поля зрения операционной системы, т. е. не числится занятым каким-либо файлом и не числится свободным (это так называемые потерянные кластеры — Lost clusters).

Потерянные кластеры можно создавать искусственно путем внесения изменений в FAT-таблицу или каталоги. Если в ячейке FAT-таблицы заменить значение, определяющее номер следующего кластера, на другое, то часть кластеров, начинающихся с того, на который указывала прежняя ссылка, будут утеряны. Если в каталоге в начало строки, определяющей характеристики файла, занести шестнадцатиричный код 00, то все кластеры, принадлежавшие этому файлу, будут рассматриваться как потерянные.

Поврежденный кластер. Операционная система в целях недопущения утраты данных исключает из употребления те кластеры магнитного диска, в которых возникают ошибки при чтении/записи данных. Эта особенность операционной системы может быть использована для сокрытия информации двумя способами. Первый основывается на том, что операционная система рассматривает кластер как одно целое, а он может состоять из нескольких секторов. Даже если в кластере повреждены не все секторы, то он все равно признается негодным. В то же время можно использовать и программы непосредственной записи в сектора магнитного диска для сокрытия информации в работоспособных секторах поврежденных кластеров.

Второй способ заключается в том, что можно пометить некоторый кластер (или их группу) как ошибочный. Поскольку операционная система не использует поврежденный кластер, то это гарантирует данным, ранее записанным в нем, полную сохранность. Единственным ограничением является отсутствие ссылок на данный кластер в FAT-таблицах и в каталогах диска. В реальности данный кластер не имеет никаких повреждений и работоспособен, поэтому в существующих ссылках на него он будет прочитан операционной системой при возникновении соответствующего запроса.

Свободное пространство в занятых кластерах. Кластер может состоять из нескольких секторов с объемом 512 байт каждый. Размер конкретного файла является величиной случайной, поэтому можно утверждать, что последний кластер занят данным файлом частично. Следова-

тельно, есть возможность занести конфиденциальную информацию в свободный остаток кластера. От прочтения эта информация будет закрыта тем, что она расположена за границей файла, а от изменения — тем, что расположена в занятом кластере. Чтобы обнаружить сведения, скрытые в свободных остатках кластеров, необходимо тщательным образом исследовать все последние кластеры, занятые файлами на данном диске.

Модификация записей в каталоге. Для сокрытия информации могут быть использованы следующие методы:

1) точка после последней буквы имени каталога приводит к невозможности его прочтения;

2) присвоение каталогу атрибут Vol ведет к его потере, метка тома должна уже существовать;

3) название каталога «...» позволяет спрятать его, в таком случае большинство программ будет считать, что это ссылка к каталогу предыдущего уровня;

4) если в записи каталога о некотором файле изменено значение размера файла в меньшую сторону, то часть информации, расположенной за пределами этого размера, не будет просматриваться многими программами;

5) если в записи каталога о некотором файле вместо первого символа имени этого файла в каталог внести код 0 (00 — в шестнадцатиричном представлении), то этот и все последующие файлы станут для операционной системы невидимыми.

Оперативное получение информации с носителя. Во время проведения следственных действий часто возникает ситуация оперативного получения информации с носителя большого объема. При этом копирование такого носителя (или создание его образа) по различным причинам может оказаться невозможным. В данном случае используются возможности ОС DOS, команды которой поддерживаются всеми последующими ОС Windows.

После запуска командного процессора командой “cmd” в командной строке необходимо набрать:

>dir d:/s > f:disk.txt, где

d: — исследуемый носитель;

/s — ключ команды dir, позволяющий получить доступ ко всем каталогам и подкаталогам на исследуемом носителе;

> — знак перенаправления вывода, указывающий место записи получаемой информации;

f: — внешний носитель, на который производится запись получаемой информации;

disk.txt — файл с результирующей информацией.

В результате выполнения команды будет создан файл большого объема, в который будет записана вся информация о файлах, каталогах и подкаталогах на исследуемом носителе. Операция записи может продолжаться до нескольких минут (в зависимости от объема каталожной информации)[1]. Чтение полученной информации можно производить в текстовом редакторе с указанием кодировки информации MS DOC.

§ 2. Файловая система NTFS

Физическая структура NTFS

NTFS, аналогично другим файловым системам, делит все полезное место на кластеры — блоки данных, используемые единовременно. NTFS поддерживает почти любые размеры кластеров — от 512 байт до 64 Кбайт, стандартом считается кластер 4 Кбайт. Диск NTFS условно делится на две части. Первые 12% диска отводятся под MFT-зону — пространство, в которое растет метафайл MFT. Запись данных в эту область невозможна, так как она зарезервирована для нефрагментированного служебного файла (MFT). Остальные 88% диска представляют собой обычное пространство для хранения файлов.

Свободное место диска включает все физически свободное место вместе с незаполненными кусками MFT-зоны. Механизм использования MFT-зоны таков: когда файлы уже нельзя записывать в обычное пространство, MFT-зона просто сокращается (в текущих версиях операционных систем ровно в два раза), освобождая место для записи файлов. При освобождении места в обычной области MFT-зона может снова расшириться. Не исключена ситуация, когда в этой зоне остались и обычные файлы.

MFT и его структура. Каждый элемент системы представляет собой файл (даже служебная информация). Главный файл NTFS — MFT (MasterFileTable) — общая таблица файлов. Он представляет собой централизованный каталог всех файлов диска и себя самого. MFT поделен на записи фиксированного размера (обычно 1 Кбайт), каждая из них соответствует какому-либо файлу. Первые 16 файлов (метафайлы) носят служебный характер и недоступны операционной системе, первый метафайл — сам MFT. Это единственная часть диска, имеющая фиксированное положение. Вторая копия первых трех записей для надежности хранится ровно посередине диска. Остальной MFT-файл может распола-

[1] Запись каталога сетевого диска сервера с библиотекой электронных изданий объемом более 150 Гб и количеством в несколько десятков тысяч файлов производилась 4 мин.

гаться (как и любой другой файл) в произвольных местах диска — восстановить его положение можно с помощью его самого через первый элемент MFT.

Метафайлы носят служебный характер. Каждый отвечает за определенный аспект работы системы. Преимущество модульного подхода заключается в поразительной гибкости. Например, на FAT-е физическое повреждение в самой области FAT фатально для функционирования всего диска, а NTFS может сместить (даже фрагментировать по диску) все свои служебные области, обойдя любые неисправности поверхности, кроме первых 16 элементов MFT.

Метафайлы находятся в корневом каталоге NTFS диска — они начинаются с символа имени "$", хотя получить какую-либо информацию о них стандартными средствами сложно. Для этих файлов указан вполне реальный размер — можно узнать, например, сколько операционная система тратит на каталогизацию всего вашего диска, посмотрев размер файла $MFT (табл. 2).

Таблица 2. **Используемые метафайлы и их назначение**

Название	Назначение
$MFT	Сам MFT
$MFTmirr	Копия первых 16 записей MFT, размещенная в середине диска
$LogFile	Файл поддержки журналирования
$Volume	Служебная информация — метка тома, версия файловой системы и т. д.
$AttrDef	Список стандартных атрибутов файлов на томе
$.	Корневой каталог
$Bitmap	Карта свободного места тома
$Boot	Загрузочный сектор (если раздел загрузочный)
$Quota	Файл, в котором записаны права пользователей на использование дискового пространства (начал работать лишь в NT5)
$Upcase	Файл — таблица соответствия строчных и прописных букв в именах файлов на текущем томе. Нужен в основном потому, что в NTFS имена файлов записываются в Unicode, что составляет 65 тыс. различных символов, искать большие и малые эквиваленты которых очень сложно

Файлы и потоки. Понятие «файл» на NTFS включает следующие элементы:

— обязательный — запись в MFT всей информации о файле, за исключением данных. Имя файла, размер, положение на диске отдельных фрагментов и т. д. Если для информации не хватает одной записи MFT, то используется несколько, причем не обязательно подряд;

— опциональный — потоки данных файла. Если файл не имеет данных, на него не расходуется свободное место диска, если файл имеет небольшой размер, тогда данные файла хранятся прямо в MFT: в оставшемся от основных данных месте в пределах одной записи MFT. Файлы, занимающие сотни байт, обычно не имеют своего физического воплощения в основной файловой области — все данные хранятся в MFT.

Каждый файл NTFS имеет абстрактное строение — у него нет как таковых данных, а есть потоки (streams). Один из потоков носит привычный смысл — данные файла, но большинство атрибутов файла — это тоже потоки. Таким образом, базовая сущность у файла только одна — номер в MFT, а все остальное опционально. Данная абстракция может использоваться для прикрепления к файлу других потоков с записями любых данных, например, информации об авторе и содержании файла (самая правая закладка в свойствах файла, просматриваемых из проводника). Дополнительные потоки не видны стандартными средствами. Наблюдаемый размер файла — размер основного потока, который содержит данные. Можно иметь файл нулевой длины, при стирании которого освободится 1 Гб свободного места, принадлежащий альтернативным данным. Имя файла может содержать любые символы, включая полный набор национальных алфавитов, так как данные представлены в Unicode — 16-битном представлении, которое дает 65 535 разных символов. Максимальная длина имени файла — 255 символов.

Создание дополнительного потока (альтернативных данных) можно осуществить следующим способом:

— запустить командный процессор командой “cmd”;

— в программе «Блокнот» для создания нового текстового файла с именем File в строке приглашения набрать: **>notepad File.txt:MyPassword.txt**.

При этом откроется программа «Блокнот» с предложением создать новый файл. В открывшемся окне можно ввести любую информацию. Завершив ввод, нужно выйти из «Блокнота», сохранив файл.

В результате описанных манипуляций будет создан основной файл File.txt, размер которого останется равным нулю. Можно менять содержимое этого файла, копировать и перемещать в другие папки, однако содержимое скрытого потока будет доступно из командной строки: **>DIR /R**.

При копировании файла с альтернативными данными на носитель с файловой системой FAT прикрепленные потоки будут потеряны.

Каталог NTFS представляет собой специфический файл, хранящий ссылки на другие файлы и каталоги, тем самым создавая иерархическое строение данных на диске. Файл каталога поделен на блоки, каждый из них содержит имя файла, базовые атрибуты и ссылку на элемент MFT, который уже предоставляет полную информацию об элементе каталога. Внутренняя структура каталога — бинарное дерево. Например, для поиска файла с данным именем в линейном каталоге FAT-а операционная система просматривает все элементы каталога, пока не найдет нужный. Бинарное дерево располагает имена файлов таким образом, чтобы поиск файла осуществлялся более быстрым способом: с помощью получения двузначных ответов на вопросы о положении файла. Вопрос, на который бинарное дерево способно дать ответ: в какой группе (относительно данного элемента) находится искомое имя? Для поиска одного файла среди 1000 FAT придется осуществить 500 сравнений (вероятно, что файл будет найден на середине поиска), а системе на основе дерева — всего около 12.

Прочитав файл каталога, можно получить информацию, которую выдает команда “dir”. Главный каталог диска — корневой — ничем не отличается от обычных каталогов, кроме специальной ссылки на него из начала метафайла MFT.

Журналирование. NTFS — отказоустойчивая система, которая может привести себя в корректное состояние при практически любых реальных сбоях. Любая современная файловая система основана на таком понятии, как *транзакция* — действие, совершаемое целиком (и корректно) или не совершаемое вообще. У NTFS не бывает промежуточных (ошибочных или некорректных) состояний — квант изменения данных совершен либо отменен. Например, при осуществлении записи данных на диск выясняется, что в намечаемое место писать невозможно из-за физического повреждения поверхности. Транзакция записи откатывается полностью, место помечается как сбойное, а данные записываются в другое место, начинается новая транзакция.

Опыт показывает, что NTFS восстанавливается в корректное состояние даже при сбоях в очень загруженные дисковой активностью моменты: вероятность потерь данных при нажатии “reset” в процессе оптимизации диска очень низка. Система восстановления NTFS гарантирует корректность файловой системы, но не данных.

Сжатие. Файлы NTFS имеют полезный атрибут — сжатый, поскольку NTFS имеет встроенную поддержку сжатия дисков. Любой файл или каталог в индивидуальном порядке может храниться на дис-

ке в сжатом виде. Сжатие осуществляется блоками по 16 кластеров, при этом используются виртуальные кластеры, что позволяет добиться интересных конфигураций: половина файла может быть сжата, а половина — нет. Такой эффект достигается благодаря тому, что хранение информации о компрессированности определенных фрагментов похоже на обычную фрагментацию файлов: например, типичная запись физической раскладки для реального (несжатого) файла:

— кластеры файла с 1-го по 43-й хранятся в кластерах диска (начиная с 400-го);

— кластеры файла с 44-го по 52-й хранятся в кластерах диска (с 8530-го).

Физическая раскладка типичного (сжатого) файла:

— кластеры файла с 1-го по 9-й хранятся в кластерах диска (начиная с 400-го);

— кластеры файла с 10-го по 16-й нигде не хранятся;

— кластеры файла с 17-го по 18-й хранятся в кластерах диска (начиная с 409-го);

— кластеры файла с 19-го по 36-й нигде не хранятся (рис. 1).

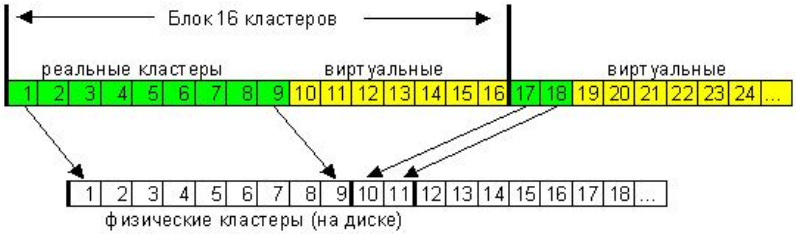

Рис. 1. Запись файла на диске формата NTFS

Сжатый файл имеет виртуальные кластеры, реальной информации в них нет. Если система видит виртуальные кластеры, она понимает, что данные предыдущего блока, кратного 16, должны быть разжаты, а получившиеся данные как раз заполнят виртуальные кластеры.

Безопасность. NTFS содержит множество средств разграничения прав объектов, которые представляют собой жесткий, но не всегда логичный набор характеристик. Права файловой системы NTFS неразрывно связаны с самой системой, но необязательны к соблюдению другой системой, если ей дать доступ к диску. Для предотвращения физического доступа существуют стандартные возможности. Система прав в текущем состоянии достаточно сложна.

HardLinks — один файл имеет два имени (несколько указателей файла-каталога или разных каталогов указывают на одну MFT-запись). Например, файл имеет имена — 1.txt и 2.txt — при удалении файла 1 останется файл 2, при удалении второго останется первый файл, т. е. с момента создания оба имени равноправны. Файл стирается тогда, когда удалено его последнее имя.

SymbolicLinks (NT5) — практичная возможность, позволяющая делать виртуальные каталоги аналогично виртуальным дискам командой "subst" в DOSe. Это можно применить для упрощения системы каталогов. Так, каталог Documentsandsettings\Administrator\Documents можно прилинковать в корневой каталог — система будет по-прежнему общаться с каталогом со сложным путем, а пользователь — с полностью эквивалентным коротким именем[2]. Для удаления связи можно воспользоваться стандартной командой "rd". Удаление связи с помощью проводника или других файловых менеджеров, не понимающих виртуальную природу каталога (например, FAR), приведет к удалению сведений, на которые дана ссылка.

Шифрование (NT5). Каждый файл или каталог может быть зашифрован, что не дает возможности прочесть его другой инсталляцией NT. В сочетании со стандартным и практически надежным паролем на загрузку самой системы эта возможность обеспечивает достаточную для большинства применений безопасность важных данных.

Особенности дефрагментации NTFS. Система NTFS подвержена фрагментации, однако внутренние структуры построены таким образом, что фрагментация не мешает быстро находить фрагменты данных.

В NT существует стандартное API дефрагментации, обладающее ограничением для перемещения блоков файлов. За один раз можно перемещать не менее 16 кластеров, причем начинаться эти кластеры должны с позиции, кратной 16 кластерам в файле:

1) в свободное место менее 16 кластеров нельзя ничего переместить (кроме сжатых файлов);

2) файл, перемещенный в другое место, оставляет после себя (на новом месте) «временно занятое место», дополняющее его по размеру до кратности 16 кластерам;

3) при попытке неправильно (не кратно 16) переместить файл результат непредсказуем.

---

[2] Для создания таких связей можно воспользоваться программой *junction* (junction.zip, 15 Кб), специалиста MarkRussinovich. Программа работает только в NT5 (как и сама возможность).

«Временно занятое место» служит для облегчения восстановления системы в случае аппаратного сбоя, освобождается через некоторое время, как правило, через 30 с.

Процесс стандартной дефрагментации с поправками на ограниченность API состоит из следующих фаз (не обязательно в таком порядке):

— «вынимание» файлов из MFT-зоны;

— дефрагментация файлов;

— дефрагментация MFT, файл подкачки (pagefile.sys) и каталогов. Возможна при перезагрузке отдельным процессом;

— перемещение файлов ближе к началу — так называемая дефрагментация свободного места.

Результат работы: первый файл оставляет хвост занятости дополнения до кратности 16, следующий — после хвоста. Через некоторое время после освобождения хвоста мы имеем «дырку» размером < 16 кластеров, которую невозможно заполнить через API дефрагментации. В результате оптимизации получаем одно пространство в конце диска и много маленьких «дырок» (< 16 кластеров) в заполненном файлами участке. При дальнейшей работе в первую очередь заполняются мелкие «дырки» (< 16 кластеров), находящиеся ближе к началу диска. Любой файл, созданный на оптимизированном диске, будет состоять из большого числа фрагментов.

Существует дефрагментатор, который игнорирует API дефрагментации — NortonSpeeddisk 5.0 для NT. Главное отличие — программа может оптимизировать диск полностью, не создавая незаполненных фрагментов свободного пространства. SpeedDisk может дефрагментировать тома NTFS с кластером более 4 Кб (в отличие от стандартного API). Сравнение файловых систем Windows FAT, FAT32 и NTFS представлено в таблице 3.

Журналирование NTFS. Очевидно, что полный undo-файл, способный откатить все операции, невозможен даже с точки зрения быстродействия. Полное журналирование применяется при работе с базами данных. В NTFS применяется журналирование логических структур, а не данных пользователя — сохранность данных не гарантируется, но корректное состояние системы будет поддерживаться. Отсутствие журналирования данных в NTFS приводит на практике к одному варианту потери данных — в случае сбоя в процессе записи никогда не удастся установить, какая часть данных записалась, а какая осталась неизменна. Операции, которые журналируются системой, — это операции со структурами самой системы, т. е. с файлами и каталогами: добавление файлов, переименование, перенос, создание и удаление (освобождение свободного места), дефрагментация.

Таблица 3. **Файловые системы Windows**

Характеристика	FAT	FAT32	NTFS
Системы, ее поддерживающие	DOS, Windows 9X, NT всех версий	Windows 98, NT5	NT4, NT5
Максимальный размер тома	2 Гбайт	Практически неограничен	Практически неограничен
Максимальное число файлов на томе	Примерно 65 тыс.	Практически не ограничено	Практически не ограничено
Имя файла	С поддержкой длинных имен — 255 символов, системный набор символов	С поддержкой длинных имен — 255 символов, системный набор символов	255 символов, любые символы любых алфавитов (65 тыс. разных начертаний)
Возможные атрибуты файла	Базовый набор	Базовый набор	Любые пожелания производителей ПО
Безопасность	Нет	Нет	Начиная с NT5.0 встроена возможность физически шифровать данные
Сжатие	Нет	Нет	Да
Устойчивость к сбоям	Средняя (система слишком проста)	Плохая (средства оптимизации по скорости привели к появлению слабых по надежности мест)	Полная — автоматическое восстановление системы при любых сбоях (не считая физических ошибок записи, когда пишется одно, а на самом деле записывается другое)
Экономичность	Минимальная (огромные размеры кластеров на больших дисках)	Улучшена за счет уменьшения размеров кластеров	Максимальная — очень эффективная и разнообразная система хранения данных
Быстродействие	Высокое для малого числа файлов, но быстро уменьшается с появлением большого количества файлов в каталогах. Результат: для слабо заполненных дисков — максимальное, для заполненных — плохое	Полностью аналогично FAT, но на дисках большого размера (десятки ГБ) начинаются проблемы с общей организацией данных	Система не очень эффективна для малых и простых разделов (до 1 Гб), но работа с огромными массивами данных и внушительными каталогами организована эффективно и превосходит по скорости другие системы

Отложенная запись и контрольные точки журналирования

Современная система для ускорения файловых операций вынуждена использовать кэширование. Отложенная запись — принцип кэширования, при котором данные, предназначенные для записи на диск, определенное время находятся в кэше и лишь в свободное от других занятий время сохраняются физически. Отложенная запись существенно повышает эффективность дисковых операций, так как кэширование группирует множество операций в одну, что особенно важно при записи в компактные участки диска. Еще один плюс отложенной записи — не мешать более нужным операциям чтения, осуществлять запись только тогда, когда система свободна и ей не требуется доступ к диску для других нужд. Однако откладывание записи не исключает потерю данных, которые находились в очереди на физическую запись и не успели записаться на диск до сбоя. Происходит рассогласование времени записи: какие-то служебные области могут быть обновлены, а какие-то смежные по смыслу — еще нет, так как их обновление могло отложиться и не состояться по причине сбоя.

NTFS справляется с такими проблемами посредством смысловой интеграции операций отложенной записи и ведения журнала. При попытке начать журналируемую операцию в лог тут же записывается намерение: например, стереть файл. Это случается без задержек — на данном этапе отложенная запись не работает — это плата за присутствие журналирования, которой нельзя избежать. Все остальные операции идут в задержанном режиме, т. е. они могут состояться частично (и не всегда в том же порядке) или не состояться вообще. Единственная задержанная операция, работа которой несколько отличается от простой записи, — запись в лог об удачном завершении предыдущих транзакций — так называемая контрольная точка. Через определенные промежутки времени (обычно через каждые несколько секунд) система в обязательном порядке сбрасывает абсолютно все задержанные операции на диск. После произведения этой операции в журнал записывается простейшая запись — контрольная точка — которая говорит о том, что все предыдущие операции выполнены корректно на всех уровнях (на логическом и физическом).

Программный RAID. Журналирование NTFS не защищает от сбоев с потерей пользовательской информации. NT предлагает несколько вариантов создания систем, где в разумных условиях гарантируется абсолютно все. Можно использовать и большее число дисков для обеспечения не повышенной надежности, а, наоборот, повышенной скорости (или того и другого одновременно).

RAID (Redundant Array of Inexpensive Disks) — избыточный массив недорогих дисков. Технология, заключающаяся в одновременном использовании нескольких дисковых устройств для обеспечения характеристик надежности или скорости, отсутствующих у накопителей в отдельности. Windows NT поддерживает на программном уровне три уровня RAID (стратегии работы дисковых массивов):

— RAID 0 — параллельные диски;
— RAID 1 — зеркальные диски;
— RAID 5 — параллельные диски с четностью.

§ 3. Программы восстановления информации после удаления

Восстановление данных с носителей

Восстановление данных с жесткого диска, флеш-накопителей и карт памяти является непростой операцией. Во многих случаях можно попробовать восстановить важные данные. При грамотном подходе это не повлечет усложнения процесса восстановления.

Recuva[3] — самая известная бесплатная программа для восстановления данных. Данное программное обеспечение позволяет легко восстановить удаленные файлы, искать определенные типы файлов (например, фотографии, которые были на карте памяти фотоаппарата). Программа проста в использовании (для восстановления данных предусмотрен удобный мастер), однако ее функциональность оставляет желать лучшего. Уверенно восстанавливаются лишь те файлы, которые были удалены, и носитель после этого вообще не использовался. Если носитель был отформатирован, то восстановить данные с него не получится. Программа не справится и в случаях, когда компьютер сообщает: «диск не отформатирован».

Программа ***UndeletePlus***[4] — простое программное обеспечение, которое предназначено для восстановления именно удаленных файлов. Программа работает со всеми носителями. Работа по восстановлению происходит с помощью мастера. На первом этапе необходимо будет выбрать, что именно произошло: файлы были удалены, диск был отформатирован, были повреждены разделы диска или что-то еще (причем в последнем случае программа не справится). После этого следует указать, какие файлы были утеряны: фотографии, документы и т. д. Рекоменду-

[3] URL: http://remontka.pro/recuva-file-recovery/ (дата обращения: 15.11.2015).
[4] URL: http://remontka.pro/file-recovery-undelete-plus/ (дата обращения: 16.12.2015).

ется использовать данную программу только для восстановления недавно удаленных файлов.

R-studio[5] — одна из лучших программ для восстановления данных. Отметим, что она является платной. Возможности программы:

— восстановление данных с жестких дисков, карт памяти, флешек, дискет, CD и DVD;

— восстановление RAID массивов (в том числе RAID 6);

— восстановление поврежденных жестких дисков;

— восстановление переформатированных разделов;

— поддержка разделов Windows (FAT, NTFS), Linux и Mac OS.

Это профессиональная программа, позволяющая восстановить данные, потерянные по разным причинам: форматирование, повреждение, удаление файлов. Она игнорирует сообщения операционной системы о неотформатированном диске. Если операционная система не загружается, программу можно запускать с загрузочной флешки или компакт-диска.

Для восстановления удаленных файлов, фотографий, видео или контактов с Android-устройств имеются специально предназначенные программы: *Wondershare Dr. Fone*[6] и *7-Data Android Recovery*[7]. Первое из двух приложений работает практически со всеми популярными марками устройств, позволяя восстанавливать не только файлы, но и другую информацию (заметки или контакты). Вторая программа работает по тому же принципу, что и бесплатная Recuva и, по сути, делает то же самое.

Программы для восстановления данных и файлов *Recovery Software*[8]. В отличие от всех остальных программ, рассмотренных выше, представляющих решения «все в одном», разработчик Recovery Software предлагает сразу 7 отдельных продуктов, каждый из которых может быть использован для различных целей восстановления:

— *RS Partition Recovery* — восстановление данных после случайного форматирования, изменения структуры разделов жесткого диска или иного носителя, поддержка всех популярных типов файловых систем;

— *RS NTFS Recovery* — аналогичное предыдущему, но работающее только с NTFS-разделами. Поддерживается восстановление разделов и

[5] URL: http://www.r-studio.com/ (дата обращения: 14.12.2015).

[6] URL: http://remontka.pro/android-data-recovery-wondershare/ (дата обращения: 16.12.2015).

[7] URL: http://remontka.pro/android-data-recovery/ (дата обращения: 18.12.2015).

[8] URL: RecoverySoftware.ru (дата обращения: 10.22.2025).

всех данных на жестких дисках, флешках, картах памяти и иных носителей с файловой системой NTFS;

— *RS FAT Recovery* — восстановление логической структуры и данных на большинстве носителей информации, кроме NTFS;

— *RS Data Recovery* — это пакет из двух инструментов для восстановления файлов RS Photo Recovery и RS File Recovery. По заверениям разработчика, данный пакет программ подойдет практически для любого восстановления потерянных файлов. Поддерживаются жесткие диски с любыми интерфейсами подключения, любые варианты Flash-накопителей, различные типы файловых систем Windows, а также восстановление файлов со сжатых и зашифрованных разделов;

— *RS File Recovery* — составная часть описанного пакета, предназначенная для поиска и восстановления удаленных файлов, восстановления данных с поврежденных и отформатированных жестких дисков;

— *RS Photo Recovery* — программа для поиска и восстановления фотографий с карты памяти фотоаппарата или флешки. Программа не требует особых знаний и навыков для восстановления фотографий, практически все сделает сама;

— *RS File Repair* — программа для решения проблем, если после использования какой-либо программы для восстановления файлов (в частности, изображения) получается «битое» изображение: с черными областями, с непонятными цветными блоками или не открывающееся. Программа помогает восстановить поврежденные графические файлы в распространенных форматах JPG, TIFF, PNG.

Скачать программы для восстановления данных Recovery Software можно с официального сайта *recovery-software.ru*. Загруженный бесплатно продукт можно опробовать без возможности сохранения результата восстановления (но этот результат можно увидеть). После регистрации программы становится доступен ее полный функционал.

Power Data Recovery — профессиональный продукт для восстановления позволяет восстановить данные с поврежденных жестких дисков, DVD и CD, карт памяти и многих других носителей, а также в случае восстановления поврежденного раздела на жестком диске. Программой поддерживаются интерфейсы IDE, SCSI, SATA и USB.

В программе для восстановления данных Power Data Recovery присутствуют возможности для поиска потерянных разделов жестких дисков, поиска нужных типов файлов, поддерживается создание образа жесткого диска с тем, чтобы производить все операции не на физическом носителе, делая процесс восстановления безопаснее.

Примечателен удобный предварительный просмотр найденных файлов, при этом отображаются (при наличии такой возможности) оригинальные имена файлов.

Stellar Phoenix позволяет искать и восстанавливать 185 различных типов файлов с разнообразных носителей (флешки, жесткие диски, карты памяти, оптические диски), но возможности восстановления RAID не предусмотрено. Программа позволяет создать образ восстанавливаемого жесткого диска для лучшей эффективности и безопасности восстановления данных, предусмотрена удобная возможность предварительного просмотра найденных файлов. Все файлы сортируются в древовидном формате по типам, что делает работу удобнее. Восстановление данных в Stellar Phoenix по умолчанию происходит с помощью мастера, предлагающего три пункта: восстановление жесткого диска, компакт-дисков, потерянных фотографий. В дальнейшем мастер проведет через все восстановления, делая процесс простым и понятным даже начинающим пользователям.

Data Rescue PC — восстановление данных на неработающем компьютере (без загрузки операционной системы при поврежденном жестком диске). Программа может быть запущена с LiveCD и позволяет:

— восстановить любые типы файлов;

— работать с поврежденными дисками и теми, которые не монтируются в системе;

— восстановить данные после удаления, форматирования;

— восстановление RAID (после установки отдельных компонентов программы).

При профессиональном наборе функций программа проста в использовании и имеет интуитивно понятный интерфейс. С ее помощью можно не только восстановить данные, но и извлечь их из поврежденного диска, который перестал видеть Windows.

Seagate File Recovery for Windows — программа от производителя жестких дисков Seagate проста в использовании, работает не только с жесткими дисками (и не только Seagate), но и с любыми другими носителями информации, находит файлы на форматированном и неформатированном диске, а также во многих других случаях. В отличие от других программ может восстанавливать поврежденные файлы в том виде, в котором их можно прочесть: например, при восстановлении фотографий некоторым другим программным обеспечением поврежденное фото не получается открыть после восстановления. При использовании Seagate File Recovery эта фотография откроется, но, возможно, не все ее содержимое можно будет увидеть.

7-Data Recovery Suite. Программу отличает удобный и функциональный интерфейс на русском языке. Программа платная, однако можно ее скачать бесплатно с официального сайта разработчика и без каких-либо ограничений восстановить до 1 Гб различных данных. Поддерживается работа с медиа-файлами, удаленными документами, возможно восстановление данных с неправильно отформатированных или испорченных разделов жесткого диска и флешки. Продукт удобен, в подавляющем большинстве случаев исправно справляется со своей задачей. На сайте разработчика есть бета-версия программы (которая хорошо работает) для восстановления содержимого внутренней памяти Android-устройств.

§ 4. Восстановление надежно удаленных данных

При удалении файла в файловой системе меняется один атрибут, он помечается как удаленный. Содержание файла по-прежнему остается на жестком диске, его можно восстановить с помощью одной из множества платных и бесплатных программ. Для удаления файлов без возможности восстановления разработано множество утилит-шредеров, которые с помощью несложных методик перезаписывают участки диска с расположенными данными. Программы для безопасного удаления данных: Eraser 6.0.8; SDelete 1.51; Freeraser; Overwrite 0.1.5; Wipe 2.3.1; Secure Delete; CCleaner 3.03. Даже при использовании технологий восстановления со считыванием данных непосредственно с магнитных носителей восстановить удаленные файлы невозможно. Однако возможности для извлечения информации есть.

Файлы изображений. Допустим, есть папка с фотографиями, пользователь удаляет одну из них, перезаписав нужную область диска. Особенностью Windows является существование файлов Thumbs.db — специального хранилища операционной системы, где находятся эскизы изображений текущей папки[9]. При выборе режима отображения проводника «Эскизы страниц» ОС будет брать уменьшенные изображения из этого файла. Последний создается в каждой папке, в которой есть картинки, содержит уменьшенные эскизы изображений в формате JPEG (вне зависимости от формата исходного изображения).

При удалении одного из изображений файл Thumbs.db может содержать эскизы уже удаленных изображений. Для отключения кэширования эскизов в файлах Thumbs.db в Windows XP необходимо установить

[9] Thumbs.db — скрытый файл, можно просмотреть и проанализировать с помощью утилиты Thumbnail DatabaseViewer.

для ключа DisableThumbnailCache в разделе HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced значение «1». В Windows 7 этот ключ имеет имя NoThumbnailCache и находится в HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Policies\Explorer.

Файл подкачки. По мере работы с документом информация о нем попадает в различные части ОС — временную папку, реестр и т. д. Поэтому трудно отследить и удалить все связанные с файлом данные. Более того, копия файла может оказаться случайно в файле подкачки (pagefile.sys) и в своп-памяти, которые используются во время режима Hibernation (hiberfil.sys). Предсказать содержимое файла подкачки заранее нельзя.

Просмотреть или скопировать файл подкачки средствами ОС невозможно, однако можно задействовать специальные утилиты или загрузить другую ОС и получить доступ к файлу из нее.

После загрузки с LiveCD и монтирования раздела Windows с помощью утилиты Foremost[10] можно провести анализ файла подкачки /mnt/hda1/pagefile.sys. Утилита сортирует файлы по типу в разные папки. Поскольку файл подкачки перезаписывается бессистемно, возможно обнаружение любых типов файлов, с которыми работал пользователь. Не все файлы после восстановления будут доступны для чтения стандартными программами, но мелкие изображения с веб-сайтов, cookie, фрагменты документов будут доступны для последующего анализа. Возникающие ошибки некритичны для текстовых файлов, картинок, аудио, видео и программ, если не затерты первые биты заголовка файла, определяющие его тип.

Отключение файла подкачки возможно через “Control Panel- > System and Security- > System- > Advanced System Settings- > Performance- > Advanced- > Virtual Memory- > Change” и выбор опции “No paging file”. Альтернативный вариант — затирание данных в файле подкачки перед выключением компьютера, активируется при установке значения «1» ключа ClearPageFileAtShutdown в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management. Этот метод очень медленный, выключение системы будет занимать длительное время. Аналогичная ситуация с файлом hiberfil.sys, который также может быть отключен.

[10] Foremost — консольная программа умеет восстанавливать файлы, опираясь на их заголовки и внутреннюю структуру. Необходимо передать имя входного файла, в котором будет осуществляться поиск, указать директорию, куда будут сохранены все найденные данные.

Исследовать файл подкачки можно и под управлением Windows с помощью программы FTK Imager. В разделе “File- > Add Evidence Item” необходимо указать диск с файлом подкачки. На панели слева отобразится дерево каталогов, где необходимо выбрать pagefile.sys и воспользоваться функцией экспорта через контекстное меню. Файл подкачки скопируется в указанную папку, при этом никакие блокировки системы не помешают его проанализировать. Для анализа можно воспользоваться DiskDigger или PhotoRec. Первая программа проще, но вторая восстанавливает широкий круг различных форматов файлов.

Дефрагментация. При осуществлении данной операции файлы переписываются в непрерывном виде ближе к началу носителя, однако их исходные копии не затираются и будут существовать до перезаписи. Эксперимент по проверке можно провести с использованием программ WinHex для непосредственного доступа к носителю информации и DiskView от Марка Русиновича[11].

Следы магнитной записи. Это применимо к таким устройствам хранения, как жесткие диски, которые используют намагничивание области для хранения состояние бита в 1, а размагничивание — 0. Если бит, установленный в 1, сбросить в 0, он будет давать слабое магнитное поле, которое контроллер устройства распознает как 0, однако его область на самом деле размагничена не идеально. Если бит, установленный в 1, опять установить в 1, т. е. повторно намагнитить область, то магнитное поле станет сильнее.

Сравнить следующие изменения, если:

— установить бит с 0 в 1 — намагниченность средняя;

— установить бит с 1 в 1 — намагниченность выше среднего;

— установить бит с 1 в 0 — намагниченность низкая;

— установить бит с 0 в 0 — намагниченность очень низкая.

Магнитные поля у них всегда будут отличаться. По этим отличиям можно определить первоначальное состояние бита, более чувствительные устройства безошибочно распознают такие изменения. В программах уничтожения данных есть параметр — количество проходов по стиранию файлов. Для идеальной чистоты диска необходима одинаковая или хаотичная намагниченность во всех областях.

[11] Программа выводит графическую схему диска, на которой можно определить местоположение данных или узнать, какой файл занимает те или иные кластеры (для этого нужно щелкнуть на кластер мышью). Двойной щелчок позволяет получить более подробную информацию о файле, которому выделен кластер.

ГЛАВА II. ОСОБЕННОСТИ РАБОТЫ С ГРАФИКОЙ

§ 1. Форматы графических файлов

Размер файла растровой графики зависит от формата, выбранного для хранения изображения. При прочих равных условиях (размеры изображения, битовая глубина) существенное значение имеет схема сжатия изображения. Многие файлы изображений обладают собственными схемами сжатия, могут содержать и дополнительные данные краткого описания изображения для предварительного просмотра. Остановимся на растровых форматах подробнее.

BMP (BitMap) создан *Microsoft*, ориентирован на применение в операционной системе Windows. Используется для представления растровых изображений в ресурсах программ. Поддерживаются только изображения в модели RGB с глубиной цвета до 24 бит. Не поддерживаются дополнительные цветовые и альфа-каналы, контуры обтравки, управление цветом. Формат предполагает использование простейшего алгоритма сжатия *(Run Length Encoding, RLE)* без потерь информации, но этот вариант используется редко (из-за потенциальных проблем несовместимости).

***PCX (PC eXchange*)** — один из первых растровых форматов, созданных фирмой ZSoft для программы *PC Paintbrush*. Поддерживает монохромные, индексированные и полноцветные изображения модели *RGB*. Не поддерживаются дополнительные цветовые и альфа-каналы, контуры обтравки, управление цветом. Формат предполагает использование простейшего алгоритма сжатия (*Run Length Encoding, RLE*) без потерь информации. PCX почти так же прост внутри, как bmp, возможности его аналогичны *bmp*, но отсутствует поддержка *OS/2*. Просмотр *pcx* осуществляется большинством программ под *DOS*, в том числе *Norton Commander*.

***PCD (Photo CD*)** разработан фирмой *Kodak* для хранения сканированных фотографических изображений. Сканирование выполняется на специальной аппаратуре (рабочих станциях *Kodak, PIW*), а его результат

записывается на компакт-диск особого формата — *Kodak Photo CD*. Его можно просматривать с помощью промышленных видеоплееров и игровых приставок на телевизоре. На практике *Photo CD* чаще применяются в издательских технологиях как источник изображений. Большинство производителей библиотек фотоснимков используют именно этот формат на компакт-дисках. Формат *PCD* имеет ряд полезных особенностей. Файл *PCD* содержит изображение сразу в нескольких фиксированных разрешениях. Базовое (*Base*) разрешение (512×768 пикселей) используется для просмотра на телевизорах *NTSC* и *PAL*. Имеются и пониженные разрешения: *Base4, Base16*, а также более высокие: *4Base, 16Base и 64Base*. Последнее разрешение, 64Base, равное 4096×6144 пикселей, есть только на дисках стандарта *Pro Master*. Наличие в одном файле шести вариантов одного изображения не увеличивает его размер, поскольку копии высокого разрешения представлены в виде разностей с базовым. Таким образом удается избежать дублирования графической информации. Изображения на *Photo CD* представлены в особой цветовой модели *YCC*, разработанной специалистами *Kodak*, во многом она аналогична модели *Lab. YCC* тоже имеет три базовых компонента: яркостный и два хроматических. Поскольку глаз более чувствителен к яркости, чем к цвету, то половина цветовой информации отбрасывается при сканировании: на каждые два пикселя приходится только одно значение хроматических компонентов. Благодаря этому удается сократить объем графических данных и размер *PCD*-файла. Для дальнейшего уменьшения размеров файла используется обычная схема сжатия без потерь качества — *LZW*. Существуют несколько форматов *Photo CD*. Формат *Master Photo CD* содержит изображения, сканированные с обычной фотопленки формата 35 мм. Максимальное разрешение для этого типа — 16 *Base*. Профессиональным фотографам адресован формат *Master Pro Photo CD*, для которого используется пленка бóльшего формата (120 мм и 4×5 дюймов). Для полиграфических приложений предназначен формат *Print Photo CD*. Оригинал сканируется профессиональными сканерами (*Crosfield, Linotype, Scitex*) и сохраняется с несжатым разрешением 64 *Base*. Формат *Catalog Photo CD* позволяет разместить на одном диске до 4500 изображений с базовым разрешением. На мультимедийные приложения ориентирован формат *Portfolio Photo CD*. На компакт-диске такого формата можно разместить до 800 изображений, а также звук, интерактивные сценарии и т. п.

***TIFF* (*Tagged Image File Format*)** создан объединенными силами *Aldus, Microsoft* и *Next* специально для хранения сканированных изобра-

жений. Исключительная гибкость формата сделала его универсальным. *TIFF* — один из самых старых форматов, в настоящее время является самым гибким, универсальным и активно развивающимся. В нем можно хранить графику в любом режиме: от битового и индексированных цветов до *Lab, CMYK* и *RGB* (кроме дуплексов и многоканальных документов). *TIFF* — основной формат, используемый для хранения сканированных изображений, а также для размещения их в издательских системах и программах иллюстрирования. Версии формата существуют на всех компьютерных платформах, что делает его исключительно удобным для переноса растровых изображений между ними. *TIFF* поддерживает монохромные, индексированные, полутоновые и полноцветные изображения в моделях *RGB* и *CMYK* с 8- и 16-битными каналами. Он позволяет хранить обтравочные контуры, калибровочную информацию, параметры печати. Допускается использование любого количества дополнительных альфа-каналов. Дополнительные цветовые каналы не поддерживаются. Поддерживает практически любой алгоритм сжатия, но наиболее распространенным является сжатие без потерь по алгоритму *LZW (Lempel Ziv Welch),* что обеспечивает высокую степень компрессии. Компания *Ulead* в 1995 г. «приватизировала» алгоритм сжатия без потерь *LZW.*

***JPEG* (*Joint Photographic Experts Group*)** впервые реализовал новый принцип сжатия с потерями информации. Он основан на удалении из изображения той части информации, которая слабо воспринимается человеческим глазом. Изображение, лишенное избыточной информации, занимает гораздо меньше места, чем исходное. Степень сжатия, следовательно, количество удаляемой информации, плавно регулируется. Низкие степени сжатия дают лучшее качество изображения, а высокие могут существенно его ухудшить. Наиболее широко *JPEG* используется при создании изображений для электронного распространения на компакт-дисках или в сети Интернет. Компактность файлов *JPEG* делает этот формат незаменимым в тех случаях, когда размер файлов критичен, например, при их передаче по каналам связи. В полиграфии использовать его не рекомендуется, хотя формат допускает хранение цветовых профилей и контуров. *JPEG* поддерживает полутоновые и полноцветные изображения в моделях *RGB* и *CMYK*. Не поддерживаются дополнительные цветовые альфа-каналы. На рисунках с четкими границами и большими заливочными областями сильно проявляются дефекты сжатия. Особенно характерно проявление «грязи» вокруг темных линий на светлом фоне и видимых квадратных областей. Последний дефект свя-

зан с тем, что алгоритм сжатия обрабатывает изображения квадратными блоками со стороной 8 пикселей.

Разновидность *progressive JPEG* позволяет сохранять изображения с выводом за указанное количество шагов (от 3 до 5 в *Photoshop*) — сначала с маленьким разрешением (плохое качество), на следующих этапах первичное изображение перерисовывается все более качественной картинкой. Анимация или прозрачный цвет форматом не поддерживаются. Уменьшение размера файла достигается сложным математическим алгоритмом удаления информации: заказываемое качество ниже, коэффициент сжатия больше, файл меньше. Важно подобрать максимальное сжатие при минимальной потере качества. Кроме коэффициента сжатия, приходится делать выбор между типами формата (стандартный, оптимизированный или прогрессивный). JPEG — наиболее подходящий формат для размещения в сети Интернет полноцветных изображений. Вероятно, до появления мощных алгоритмов сжатия изображения без потери качества он останется ведущим форматом для представления фотографий в *Web*. Плохо, что качество теряется при каждом последующем сохранении.

Существует три подформата *jpg*: обычный, optimized (файлы несколько меньше, но не поддерживаются старыми программами) и progressive (отображение через строку, аналог interlaced в gif). Некоторые приложения позволяют хранить изображение в *jpg* в режиме *CMYK* и даже включать в файл обтравочные контуры. Однако использовать *jpg* для полиграфических нужд категорически не рекомендуется из-за взаимодействия регулярной структуры блоков 8 × 8 пикселей, получающихся в результате компрессии, с не менее регулярной структурой типографского растра, что в итоге приводит к образованию муара. Используется для хранения крупных фотографий с большим количеством плавных цветовых переходов. Нельзя сохранять одно изображение в jpg больше одного раза: слишком заметны деструктивные изменения картинки от повторного использования компрессии.

PNG (читается *пинг*) *(Portable Network Graphics)* — самый прогрессивный формат графики для сети Интернет, поддерживает полутоновые и полноцветные RGB-изображения с единственным альфа-каналом, а также индексированные и монохромные изображения без альфа-каналов. Альфа-канал служит маской прозрачности. Формат *PNG* — единственный из распространенных в сети форматов, дающий возможность получать полноцветные изображения с прозрачным фоном. Он позволяет создавать зоны прозрачности как *gif*, но может быть и полупрозрачным (просвечивать фон). *PNG* не поддерживает многоканальных изображе-

ний, цветовых профилей и контуров обтравки. Вместо *LZW* в формате png используется алгоритм *Deflate*, дающий несколько лучшие результаты. Изначально призван заменить морально устаревший *gif* в сети, но предлагает ряд новых возможностей. Это относительно молодой формат для *Web*-графики, конкурирующий с GIF. Все последние версии браузеров поддерживают его без специально подключаемых модулей.

Существует два подформата: *PNG8* и *PNG24*, цифры означают максимальную глубину цвета, возможную в подформате. В *PNG 24* реализована поддержка 256 градаций прозрачности за счет дополнительного альфа-канала с 256 градациями серого. С помощью этой функции, например, полупрозрачный логотип может выглядеть одинаково на абсолютно любом фоне. Полезные возможности png: двумерный *interlacing* (т. е. изображение проявляется постепенно не только по строкам, но и по столбцам); встроенная гамма-коррекция, позволяющая сохранять изображения, яркость которых одинакова как на *PC*, так и на компьютерах *Mac, Sun u Silicon Graphics*. Однако ни одна из функций не поддерживается существующими браузерами. *PNG8* мало распространен из-за слабой рекламы, создавался специально для Интернета в качестве замены первых двух форматов, благодаря патентной политике *Compuserve* постепенно вытесняет *GIF*. Позволяет выбирать палитру сохранения — серые полутона, 256 цветов, true color (истинные цвета). В зависимости от свойств изображения, действительно, иногда предпочтительнее, чем *GIF*. Позволяет использовать до 256 прозрачных цветов. В отличие от *GIF*, сжатие без потери качества производится по горизонтали и вертикали (алгоритм собственный, параметры тоже ненастраиваемые). Не поддерживает анимацию. Не поддержан фирмой *Microsoft*.

WBMP Wireless Bitmap (WBMP) специально оптимизирован для мобильных устройств. Описание этого формата вместе с языком разметки *WML (Wireless Markup Language)* включено в спецификацию *WAP (Wireless Application Protocol)*. Изображения *WBMP* способны создавать *Photoshop 7, Macromedia Fireworks 4* и выше. Формат поддерживает только два цвета, но можно имитировать и большее количество с помощью разброса пикселей (*dithering*). Теоретически файлы *WBMP* могут содержать анимацию. Сжатие не поддерживается, однако графический файл для *WAP* не может быть больше 1461 байта (ограничение связано с небольшим объемом памяти сотовых телефонов). Из-за скромного разрешения дисплеев мобильных устройств безопасный размер файлов ограничен форматом 90 × 24 пикселей. Немногие устройства способны отображать графику в этом формате.

PXR (Pixar) предназначен для обмена со специализированными графическими станциями *Pixar*, ориентированными на трехмерное моделирование и анимацию. Поддерживаются только полутоновые и полноцветные *RGB*-изображения с единственным альфа-каналом.

PSD (Photoshop Document) — собственный формат программы *Adobe Photoshop*. Единственный формат, поддерживающий все возможности программы. Предпочтителен для хранения промежуточных результатов редактирования изображений, так как сохраняет их послойную структуру. Все последние версии продуктов фирмы *Adobe Systems* поддерживают этот формат и позволяют импортировать файлы *Photoshop* непосредственно. К недостаткам формата можно отнести недостаточную совместимость с другими распространенными приложениями и отсутствие возможности сжатия. Поддерживаются все цветовые модели и любая глубина цвета от бело-черного до true color, сжатие без потерь. Начиная с версии 3.0 *Adobe* добавила поддержку слоев и контуров, поэтому формат версии 2.5 и ранее выделяется в отдельный подформат. Для совместимости с ним в более поздних версиях *Photoshop* имеется возможность включить режим добавления в файл одного базового слоя, в котором слиты все слои. Такие файлы читаются большинством популярных просмотрщиков, импортируются в другие графические редакторы и программы для 3D-моделирования.

FLM (Filmstrip) — собственный формат *Adobe Premier*, программы редактирования видеоинформации и создания презентаций.

***IFF* (*Amiga Interchange File Format*)** используется на компьютерах *Commodore Amiga* с программно-аппаратным комплексом *Video Toaster*. Он ориентирован на создание и обработку высококачественных видеоматериалов в реальном времени. Поддерживается некоторыми программами рисования на платформе *Windows*, например, *Deluxe Paint* фирмы *Electronic Arts*. Формат *IFF* поддерживает все типы изображений, за исключением многоканальных и полноцветных *CMYK*. Обтравочные контуры, цветовые профили и альфа-каналы не поддерживаются.

SCT (Scitex Continuous Tone) используется сканерами, фотонаборными автоматами и графическими станциями *Scitex* для получения высококачественной полиграфической продукции. Особый формат используется патентованным растеризатором Scitex. Он поддерживает полутоновые и полноцветные изображения в моделях *RGB* и *CMYK* без альфа-каналов. Обтравочные контуры и цветовые профили не поддерживаются. *Scitex* используется на этапе растрирования смеси из векторных и растровых данных в одну битовую карту, предназначенную для

high-end фотонаборных автоматов фирмы *Scitex*. Не поддерживает никаких алгоритмов сжатия.

***PCT/PICT* (*Macintosh QuickDraw Picture Format*)** — внутренний формат операционной системы *Mac* (аналог *bmp*). Способен нести растровую и векторную информацию, текст и даже звук. Гибкость формата подтверждает эффективность использования *Mac* при работе с мультимедиа. Изображение может храниться как в *RGB*, так и в *CMYK*, причем глубина цвета варьируется от индексированных цветов до true color; реализован алгоритм компрессии без потерь *RLE*. Формат *pict* открывается всеми приложениями, разработанными для *Mac* (*QuickTime*, *Photoshop* и т. д.).

RAW не поддерживает ничего. Не хранятся даже данные о количестве каналов, глубине цвета и разрешении, во время открытия приходится вводить эти параметры вручную (по памяти). Изображение хранится просто как поток пикселей с фиксированным заголовком, куда впоследствии можно поместить любую текстовую информацию. Размер заголовка в байтах тоже придется указывать при открытии картинки в этом формате. Обладает мультиплатформенностью и совместимостью со всеми программами, однако не каждый графический редактор или просмотрщик поддерживает *raw*.

***TGA* (*Targa*)** создан специально для работы с графическим акселератором *TrueVision*. Этот акселератор широко используется приложениями на платформе *DOS*. Формат поддерживает 24-битные и 32-битные *RGB*-изображения с одним альфа-каналом, а также полутоновые, индексированные и 16-битные *RGB* изображения без альфа-каналов. Обтравочные контуры и цветовые профили не поддерживаются. Использует алгоритм компрессии без потерь *RLE*. Файлы формата *targa* часто применялись *DOS* версией *3DStudio Max* для хранения текстур.

FPX (FlashPix) был разработан фирмой *Kodak*. *FlashPix* поддерживает несколько копий с разным разрешением в одном файле. Ориентирован на полиграфию с изображениями в десятки и сотни мегабайт. Их приведение к нужному размеру занимает гораздо больше времени, чем просто считывание копии с нужным разрешением, размер файлов в предпечатной подготовке роли не играет. *FlashPix* обладает встроенной системой защиты изображений с помощью водяных знаков. Формат встречается нечасто, немногие программы умеют с ним работать.

PXR Pixar — редкий формат, применяется исключительно на *high-end* графических станциях *Pixar*, предназначенных для профессиональной трехмерной анимации. Его возможности невелики: отсутствие компрессии, поддержка модели *RGB*, градаций серого и одного альфа-канала.

ICO — формат мелких картинок (иконок) в *WWW*. Картинки используются браузерами для маркировки *Web*-проектов в строке *URL* и в избранном. Поддерживается и используется программками для создания иконок типа *IconXP*.

В таблице 4 приведены размеры файлов в байтах в различных графических форматах. Для сохранения в другом формате использовалась программа *Adobe Photoshop* 4.0. При сохранении в формате JPEG использовались различные степени сжатия (*JPG* 2, *JPG* 4, *JPG* 8), чем больше число, тем выше качество и, соответственно, размер файлов.

Таблица 4. **Размеры файлов в различных графических форматах, байт**

Файл	Графический формат				
	Asia	Paint Windows	Sunset	Копия экрана	Paint Windows
Размер файла	640 × 430 24 бит	800 × 600 24 бит	640 × 480 24 бит	800 × 600 24 бит	800 × 600 2бит
EPS Photoshop	2305769	3997119	546930	4000397	158532
PXI Pixel Paint	–	–	–	–	127655
PCX	905409	152532	189128	498615	38158
TIF	830528	1444530	195772	1446106	64194
SCT Scitex	827648	1442048	194048	1442048	–
PXR Pixar	827392	1441792	193536	1441792	–
BMP	825656	1440054	192056	1440056	60062
BMP LZW	–	–	192054	–	–
TGA Targa	825644	1440044	128044	–	–
RAW	825600	1440000	192000	1440000	–
PSD Photoshop	823718	195644	192453	1032168	40407
PCT 32 bit	815040	195644	187620	479742	–
PCT 16 bit	475914	170836	–	–	34680
IFF Amiga	680494	792338	172304	768198	33158
TIF LZW	669178	101012	89234	229514	21030
PNG	627061	60526	144008	158054	–
TGA	550444	–	–	–	–
PDF	198976	529187	34114	325514	–
JPG 1	327806	112965	–	–	–
JPG 2	–	–	–	110951	–
JPG 4	–	–	10217	–	–
JPG 8	–	385880	–	227186	–
GIF	–	–	–	–	17118

Векторные форматы

EPS (Encapsulated PostScript). Благодаря своей надежности, совместимости со многими программами и платформами, настраиваемым параметрам формат является выбором большинства профессионалов в области полиграфии. Он предназначен для переноса готовых изображений в программы верстки, поддерживает цветовые модели *CMYK, RGB,* дуплексы и содержит готовые команды устройству вывода. В *EPS* можно сохранить информацию о треппинге, типографском растре, внедренных шрифтах и обтравочных контурах. Данные сохраняются тремя способами: *ASCII* (медленный, но наиболее совместимый), *Binary* (быстрый и компактный), *JPEG* (быстрый, но с потерями качества и плохой совместимостью). При сохранении в *EPS* можно указать формат и глубину цвета эскиза, который для ускорения работы будет выводиться на экран в программах верстки вместо большого оригинала.

FLA — внутренний формат программы для создания интерактивной анимации *Flash.*

SWF — формат публикации *Flash* для отображения на разных платформах.

§ 2. Технологии обработки графических файлов

Еще в середине XX в. обработка изображений была аналоговой и выполнялась оптическими устройствами. Подобные методы до сих пор важны, например, в голографии. С ростом производительности компьютеров они вытеснялись методами цифровой обработки изображений, такой способ в настоящее время является самостоятельной быстроразвивающейся областью науки и техники. За последнее десятилетие область применения цифровой обработки изображений значительно расширилась за счет повышения производительности ЭВМ и технических средств. Основная сложность для средств и методов обработки заключается в сверхбольших объемах информации с высоким разрешением. Исправить ситуацию можно созданием комплексной автоматизации ввода, обработки, хранения, визуализации и вывода изображений, что позволит сократить разрыв между эффективными методами получения изображений и рутинными, ручными способами их обработки.

Программные средства обработки цифровых фотоснимков предназначены для пользователей разного уровня подготовки: от профессионалов до начинающих.

Программа Photo Cleaner служит для улучшения качества цифровых фотографий, полученных со сканера изображений, и т. п. В отли-

чие от других подобных программ, все изменения производятся в автоматическом режиме, хотя программа и имеет небольшое количество настроек: можно изменять размер обрабатываемых изображений, добавлять границы, подписи под фотографиями и т. д. Есть функция обработки сразу нескольких фотографий, генерации фотоальбома в виде HTML-страниц. Программа корректирует цветность, яркость, резкость, уровни цветов.

Студия эффектов Программа от AMS Software служит для преобразования фотографий при помощи уникальных фильтров, присутствуют профессиональные эффекты для фото. Программа позволяет добавлять свечение и туман, генерировать эффекты дождя, снега, молнии и звездного неба, создавать эффект старинного фото и рисунка карандашом, а также мозаики, гравюры, книжной иллюстрации и многое другое. Студия эффектов включает ряд фильтров, например, выжигание по дереву, кубизм и фотомонтаж, возможно стильное оформление фотографий при помощи рамок и масок, добавление надписей и украшений.

Mediachance Dynamic Auto-Painter позволяет преобразовывать фотографии в картины, используя имитацию техники живописи знаменитых художников: Климта, Моне, Ван Гога и др. Возможна имитация техники рисования карандашом, письма пастелью, маслом, гуашью, акварелью.

Программа не изменяет фотографию, а использует изображение в качестве оригинала, с которого автоматически рисует новое изображение, применяя соответствующие кисти и стили. Разрешение готового изображения не зависит от разрешения оригинала, может превышать его в несколько раз. Функция *Real Canvas* моделирует реальную фактуру холста и красок. Готовые изображения похожи на живопись даже в небольшом разрешении.

ФотоСАЛОН — программа для стильного оформления фотографий, позволяет наложить красивую рамку, создать поздравительную открытку или коллаж. Программа включает все необходимые функции для обработки цифровых фотографий: автоматическое улучшение и редактирование, создание спецэффектов, календарей, обрамление, добавление украшений и надписей. Комплект программы включает более трехсот различных вариантов оформления. Программа имеет настраиваемый интерфейс и проста в освоении.

Picget PhotoShine позволяет вставить выбранную фотографию в один из «звездных» шаблонов. Фотоснимок преобразуется в изображение в телевизоре, на обложке журнала, на рекламных постерах либо на долларовых купюрах.

Adobe Photoshop имеет набор инструментов для работы с растровой графикой. Основное направление этой программы — работа с цифровыми изображениями: цветокоррекция, ретушь, фотомонтаж и пр. Можно использовать для дизайна веб-сайта, создания постера или анимированного баннера для блога.

Adobe Photoshop Lightroom. Основная функция программы — пакетная обработка фотографий, возможность применять фильтры цвето(коррекции, коррекции теней, шумов, резкости и пр.) к многочисленным фотографиям. Особенность программы — работа с изображениями в формате RAW(NEF) без внутреннего сжатия камерой, возможно применение различных методов обработки без потери качества снимка. Этот формат хранит в себе всю информацию о снимке, с помощью которой можно легко изменять экспозицию, убирать шумы и увеличивать резкость изображения.

Adobe Photoshop Lightroom позволяет экспортировать обработанные изображения в Adobe Photoshop, что дает возможность еще более качественно обрабатывать фото.

NIK SOFTWARE COLOR EFEX PRO. В комплекте программы присутствуют 55 фильтров и более 300 эффектов для добавления в снимки. Доступны действия от простой ретуши до отбеливания зубов.

IMAGENOMIC PORTRAITURE & NOISEWARE PROFESSIONAL компании Imagenomic — инструменты для ретуширования кожи (Portraiture) и снижения уровня цифрового шума (Noiseware Professional).

Возможности монтажа

Фотомонтаж (коллаж) — процесс и результат создания изображений, составленных из частей различных фотографий. Фотомонтаж широко применяется при изготовлении плакатов, реклам, политических карикатур и пр. При изготовлении фотомонтажа самым трудным является подбор цветов и яркости, определение масштаба отдельных частей и их выравнивание в изображении.

При ***аналоговом способе фотомонтажа*** из фотографий вырезают нужные части изображения, подгоняют их путем увеличения под необходимый масштаб, склеивают на листе бумаги, ретушируют, затем переснимают. Другой вариант — совмещение нескольких негативов при печати.

С развитием компьютерной техники появился и арсенал программного обеспечения для фотомонтажа. Наиболее распространенные программы для фотомонтажа — Adobe Photoshop, Corel Photo-Paint, GIMP.

Цифровая фотография позволяет сразу использовать отснятый материал для цифрового фотомонтажа (без предварительного сканирования). Профессиональное использование современных средств обработки цифровых изображений позволяет запечатлеть человека в образе различных исторических персонажей, вписать в полотна прославленных художников, изобразить его на другой планете или в другой исторической эпохе. Есть возможность удалить или добавить разнообразные элементы в конечном изображении: от текста и виньеток до отдельных лиц на снимке. Фотографии могут быть оформлены в едином стиле, в одинаковых рамках, стилизованы под разные периоды (черно-белые с резным краем, сепия, цветные).

При кажущейся простоте современный фотомонтаж — это серьезная и сложная работа, которая, помимо профессионального умения, требует наличия специальных знаний, построения композиции, теории света, сочетания и совместимости цветов и художественного вкуса.

Традиционный фотомонтаж представлял собой репродукцию совмещенных фрагментов ранее изготовленных снимков. Поэтому распознавание фотомонтажа производилось на основе изучения композиции изображения и пропорциональности его частей, освещения объектов, соотношения плотностей почернения, резкости и зернистости изображения, наличия ретуши, маскирующей границы объектов, и пр. Проводилось изучение четырех основных аспектов. Рассмотрим их:

1) передача *перспективы* как возможное искажение мотива: для реалистичных результатов все объекты должны быть сфотографированы приблизительно при одном и том же фокусном расстоянии;

2) *ракурс*, с которого сфотографированы все объекты, должен совпадать. Сложно сделать реалистичный монтаж фотографии человека, снятого с балкона, с фотографией здания, сфотографированного снизу;

3) неправильное *освещение* не всегда может быть явным, но на фото заметно, что что-то неправильно. Тени от предметов на пейзаже, падающие вправо, и тень от вмонтированной фигуры, падающая влево, вызывают чувство дискомфорта у рассматривающего фотографию;

4) неверно подобранный *цвет* часто портит фотомонтажи, удачные в остальных аспектах.

В настоящее время точная обработка деталей до единичного пикселя, масштабирование по размеру, коррекция цветовой гаммы и направленности освещения монтированных объектов, изменение яркости и контрастности — вот неполный перечень возможных операций для улучшения качества фотографии. Для создания естественности изображения объектов (наклон и поворот головы, улыбка, положение рук и т. д.) могут

быть использованы результаты предварительной видеосъемки на цифровую камеру. Указанные операции могут производиться как над полным изображением, так и над отдельными фрагментами. Графические редакторы позволяют масштабировать изображение и производить операции над пикселями, не превышающими размер зерна на традиционной фотопленке.

Результат будет получен при высококачественной распечатке на специальной бумаге с использованием струйной и лазерной техники цветной печати. При идентификационном исследовании фотографических материалов особенности технологии печати позволяют по качеству бумаги, используемым чернилам, порошкам, по иным параметрам определить, что данная продукция изготовлена нестандартным фотопроцессом. Цифровая фотопечать, выполняемая на специальном оборудовании, дает более качественный результат, внешне неотличимый от традиционной фотографии.

Для изготовления качественного фотомонтажа квалифицированный злоумышленник может создать негативное изображение на прозрачной пленке, которое в дальнейшем может быть использовано для контактной фотопечати. С применением современного струйного фотопринтера (с разрешением 1200–2800 точек на дюйм) может быть изготовлен негатив для стандартного процесса печати с использованием фотоувеличителя.

При создании негативного изображения на пленке может быть использован процесс репродуцирования с качественного изображения большого формата. Репродуцированное изображение от натурного снимка отличается наличием специфических признаков, указанных ранее. Однако отсутствие названных признаков не является основанием для категорического вывода, поскольку на высококачественной репродукции они могут отсутствовать, а признаки, специфические для натурных снимков, пока еще не определены.

§ 3. Возможности определения фальсификации фотографий

Как еще можно убедиться в подлинности изображения? Раньше с помощью фотографий люди фиксировали события, в настоящее время нужно подходить к фотографиям более критично. Необходимо проводить работу для установления подлинности изображения: сравнивать несколько фотографий одного события, снятых разными людьми. Подлинность снимков подтверждает одинаковость кадров, сделанных независимыми фотографами. Фотомонтаж используют и для создания компрометирующих снимков, поэтому фототехническая экспертиза остается востребованной до сих пор.

Фототехническая экспертиза, одна из традиционных методик экспертного исследования, включает три направления:

1) идентификационное исследование фотографических изображений (идентификация фотоаппарата по негативу);

2) диагностическое исследование фотографических изображений;

3) идентификационное исследование фотографических материалов (определение типа и вида материала).

Современное развитие компьютерных технологий ставит под сомнение дальнейшее существование и развитие некоторых из них.

При традиционном диагностическом исследовании фотографических изображений эксперт должен определить соблюдение технологических правил съемки и лабораторной обработки светочувствительных материалов. Эксперт, отмечая недостатки изображения, на основе знания фотографических процессов объясняет их происхождение. Наличие на снимках ретуши и способы ее нанесения устанавливаются в результате исследования снимка при некотором увеличении. Репродукции и натурные снимки различают по наличию специфических признаков, возникающих при репродуцировании: воспроизведенные дефекты оригинала, неравномерная резкость изображения, блики от прижимного стекла, отображение источников освещения, растровые точки в рисунке и т. п.

Обратим внимание на сложность (а в некоторых случаях и невозможность) получения определенных результатов при проведении фототехнической экспертизы. По этой причине отношение к фотодокументам, полученным из недостоверных источников, а также предлагаемым в качестве доказательств, должно быть критичным. Необходимо понимать, что качество предварительной обработки фотоматериалов на компьютере может быть настолько высоким, что эксперт при проведении фототехнической экспертизы не сможет определить наличие ретуши или монтажа. При проведении экспертизы необходимо обратить внимание на наличие особых примет, естественность позы, внешний вид (одежда), окружающий пейзаж и т. д., на косвенные детали, по которым может быть определена предварительная обработка фотоматериалов на персональном компьютере.

Для распознавания обработки цифрового фото создаются специальные программы, проводятся компьютерно-технические экспертизы. В качестве примера можно привести экспертное исследование фотографий незаконченных строительных объектов, в ходе которого требовалось установить возможность фотомонтажа и решить вопрос о времени получения снимков. Эксперту была представлена и флеш-карта, содержащая несколько графических файлов формата JPEG.

Осмотром и микроскопическим исследованием фотоснимков было установлено, что все изображения являются цветными, среднеконтрастными, с удовлетворительной резкостью, яркостью и передачей полутонов. Изображения объектов на снимках имели пропорциональные перспективные искажения, общая картина распределения освещенности кадров изображений выглядела естественной, наблюдаемые на отдельных участках каждого из снимков глубокие тени образованы одним направленным источником света. На светотеневых границах изображений резких переходов, локальных участков со светлыми полосами на изображениях (контурных ореолов), а также ступенчатой структуры прямолинейных контрастных участков изображений не обнаружено. Другими словами, изученные фотоизображения не содержали каких-либо признаков, свидетельствующих об использовании приемов фотомонтажа (изготовления репродукций фотографических изображений, смонтированных из двух или более самостоятельных изображений).

С этой же целью изучались изображения и компьютерных файлов. Установлено, что электронные изображения полностью (во всех визуально наблюдаемых деталях) совпадают с изображениями на фотоснимках. Соответственно, отсутствие фотомонтажа в изображениях на листах бумаги характерно и для изображений в электронном виде.

Дополнительно изучались гистограммы изображений, содержащихся в исследуемых файлах. Обнаружено, что в большинстве изображений они имели высокий пик ближе к средней части графика и равномерное (небольшого уровня) распределение пикселей в левой «темновой» зоне гистограммы. В правой части гистограммы, соответствующей светлым частям изображений, число пикселей было незначительным или вовсе отсутствовало. В цифровой фотографии подобное изображение считается «сырым», необработанным, поскольку для качественного отображения всех деталей изображения его тоновый диапазон, демонстрируемый гистограммой, должен быть приведен к норме, т. е. занимать весь участок гистограммы. Однако при растяжке слишком узкого тонового диапазона на гистограмме изображения появляются характерные вертикальные белые полосы — так называемые просечки, которые в данном случае отсутствовали. Анализ гистограмм исследуемых изображений позволил обоснованно судить о том, что представленные компьютерные файлы какому-либо редактированию с использованием программных средств обработки изображений не подвергались.

В дополнение к описанным методикам следует отнести и детальное (пиксельное) исследование файла изображения. При создании коллажа

из нескольких источников очень сложно добиться равномерного размера пикселей изображения: при увеличении вносимых элементов их пикселизация будет отличаться от базового изображения.

Еще один способ подтверждения подлинности фотографии — исследование EXIF-информации. При записи камерой изображения в формате JPEG сохраняются особенности, свойственные именно этой камере. Метаданные и данные EXIF сохраняют информацию о камере: фокусное расстояние, использование вспышки, время снимка. Камеры могут сохранять координаты, где было снято фото. Производители камер принимают решение о способе сжатия картинки при помощи стандарта JPEG. При этом необходимо настроить сотни параметров. Стандарт EXIF определяет информацию об изображении, которые камера автоматически сохраняет вместе с самим изображением. При изменении изображения в программе или Интернете EXIF фотографии не может остаться прежним. EXIF-информация файла меняется даже при открытии файла программой-просмотрщиком. EXIF-информацию можно увидеть либо в свойствах файла, либо с использованием специальных программ (типа свободно распространяемой EXIFViewer).

Специальные программы типа FourMatch* читают метаданные, данные стандарта EXIF, параметры, свойственные каждой модели камеры, которые обычный человек не может просто так изменить. Например, программа FourMatch использует технику определения внесения изменений (загрузка в соцсети, открытие изображения в программе-редакторе или программе по управлению фотографиями).

Эту информацию можно модифицировать после изменения изображения. Цифровое изображение остается компьютерным файлом с особенным методом записи информации, что определяет возможность копирования и модификации служебной информации в цифровом виде. Квалифицированный специалист может произвести последовательность операций: копирование EXIF-информации исходного файла > коррекция графического изображения > восстановление из копии EXIF-информации. Результатом данных манипуляций будет скорректированный файл с исходной EXIF-информацией, что может ввести в заблуждение эксперта. Можно идеально сфальсифицировать фото, но в этом случае следует применить традиционные методики определения фотомонтажа, например, несоответствие в освещении. Технологии не могут однозначно определить сфальсифицированное фото.

---

* *Сайт* компании Fourandsix Technologies. URL: http://www.Fourandsix.com (дата обращения: 15.11.2015).

ГЛАВА III. МЕХАНИЗМЫ ЛОГИРОВАНИЯ ИНФОРМАЦИИ

§ 1. Типы логов. Конфигурирование логирования информации

Одна из функций системного администратора или специалиста по безопасности — анализ того, что происходит на конкретном компьютере пользователя и в локальной сети. Основным инструментом технического выполнения задачи является заложенное разработчиками программных продуктов логирование информации. Для понимания информации лог-файлов различных приложений необходимо иметь представление о предметной области изучаемой программы, поскольку запись информации в логи, как и сами программы, не подчиняется определенному стандарту, а зависит только от производителя. Соответственно, интерпретировать такую информацию необходимо с учетом специфики и рекомендаций производителя. Для прочтения информации из логов иногда достаточно простого текстового редактора, но встречаются иные ситуации, когда для просмотра файла надо знать особенности структуры различных лог-файлов.

Существующие типы логов можно разделить на три класса:

1. Текстовые логи используются часто. Отдельное событие представляет собой отдельную строку. Например, известный *Symantec Antivirus* или *Linux Syslog*. Способ хорош как с точки зрения реализации — легко наладить такое логирование в коде большинства языков программирования, так и со стороны использования — читать такой лог можно любым текстовым редактором.

2. Более сложный случай — это логи, в которых отдельное событие представляет собой несколько строк. К такому типу можно отнести логи в формате XML (либо сходные форматы данных). Такой лог более сложен для анализа, поскольку каждое событие может представлять набор мелких записей. Для чтения данных файлов часто используется специальная программа (из-за сложности интерпретации зависимых событий).

3. Бинарный лог представляет собой самый нечитаемый тип. Для работы с ним нужна специальная программа (обычно того же производителя, что и приложение, которое пишет такой лог). Бинарный лог представляет собой последовательно сбрасываемые в файл структуры, разделяемые символом. При наличии технической документации от производителя с описанием формата возможно существование программ для интерпретации логов, но при закрытом формате файла анализ возможен только встроенными средствами.

Приложения, которые используют базы данных либо сами являются системами управления базами данных (далее — СУБД), часто используют базу данных в качестве хранилища логов. Как правило, это отдельная таблица базы данных, каждая строка которой является самостоятельным событием. Такое логирование может отрицательно сказаться на общей производительности базы данных, так как логирование в базу данных иногда бывает довольно интенсивным (например, MS SQL Server 2000/2005 успевает писать логи в C2 Audit несколько десятков записей в секунду). Конфигурирование приложения определяет его работу, однако использование базы данных для логирования информации, касающейся транзакций и безопасности, не отменяет наличия файловых логов в остальных сервисах, входящих в СУБД.

Обычно процесс логирования незаметен. Запись лога производится в предусмотренной производителем конфигурации, которая не вызывает проблем у пользователя. Однако возможны следующие ситуации:

— понижение производительности из-за постоянной записи информации в логи (на жесткий диск);

— проблемы со свободным местом на жестком диске;

— влияние на производительность системы.

Часто инсталляционная программа требует точных указаний о конфигурации логирования либо выключает логирование полностью. Рассмотрим типичные функции настройки.

1. Имя файла, директория или полный путь к тому файлу, в который пишется лог.

2. Критерии замены лога (Log Rotation) в случае его разрастания:

— каждый день (неделю, месяц и т. д.) система использует новый лог-файл. Если смена лог-файлов связана с каким-либо исчислением времени (каждый день, каждый год и т. п.), то в имени используется время (дата и время, только дата, иногда какая-нибудь производная) создания или финального закрытия (финализация) данного лог-файла. Если система использует уникальное имя (имя с датой, временем или их производной можно считать уникальным, так как время монотонно

возрастает), то такие логи обычно не очищаются системой. Например, Symantec Antivirus или Tivoli Access Manager for e-Business используют лог-файлы, которые хранят в своем имени время смены лог-файла;

— смена файла происходит по достижении им определенного размера, старый файл сохраняется некоторое время или удаляется по решению пользователя. Например, Linux (UNIX) Syslog, который позволяет настраивать как размер файла, так и количество используемых файлов;

— смена файла происходит одновременно с перезапуском сервиса, который пишет лог. При отсутствии перезапуска это приводит к большому размеру лог-файла. Используется, например, HP Tru64 UNIX (ограничение довольно велико — около 300 Мб);

— частота сброса информации в файл, например, Tivoli Access Manager for e-Business при грамотной настройке уменьшает число обращений к жесткому диску от логирующей программы, однако его модификация может серьезно снизить производительность сервера.

3. Набор событий, которые логируются, почти всегда можно настраивать. Например, из всех транзакций в базе данных выбираются содержащие угрозы (с точки зрения безопасности). В этом случае снижается нагрузка на сервер, но остается учет реально необходимых событий: попыток авторизации, попыток доступа к файлам, изменение системных настроек и т. п. Обычно производитель предоставляет свои профили логирования: от полного выключения до полного логирования всего происходящего. Довольно часто есть возможность указать даже не профиль, а настройки логирования для каждого конкретного события (например, такая возможность есть в MS SQL Server C2 Audit). Такие настройки позволяют сделать гибкое логирование информации, которая нужна в конкретном случае, но настройка логируемых событий встречается не во всех программах.

Отметим, что указанные основные функции часто расширяются производителями программ под собственные нужды. Разрабатываются новые форматы хранения данных, новые методы и стандарты представления данных, улучшаются производительность и универсальность систем логирования.

§ 2. Логирование событий в Windows 7

Операционная система Windows 7 постоянно следит за различными событиями, достойными внимания, возникающими в системе. В Microsoft Windows ***событие (event)*** — это любое происшествие в операционной системе, которое записывается в журнал или требует уведомления пользователей (администраторов), служба, которая не хочет запускаться, установка

устройства или ошибка в работе приложения. События регистрируются и сохраняются в журналах событий Windows, предоставляют хронологические сведения, помогающие вести мониторинг системы, поддерживать ее безопасность, устранять ошибки и выполнять диагностику.

Программа «Просмотр событий» представляет собой оснастку консоли управления Microsoft (MMC), предназначена для просмотра и управления журналами событий. Служба Windows, управляющая протоколированием событий, называется «Журнал событий». При помощи программы «Просмотр событий» (рис. 2) можно выполнять следующие действия:

— просматривать события определенных журналов;

— применять фильтры событий и сохранять их для последующего использования в виде настраиваемых представлений;

— создавать подписки на события и управлять ими;

— назначать выполнение конкретных действий на возникновение определенного события.

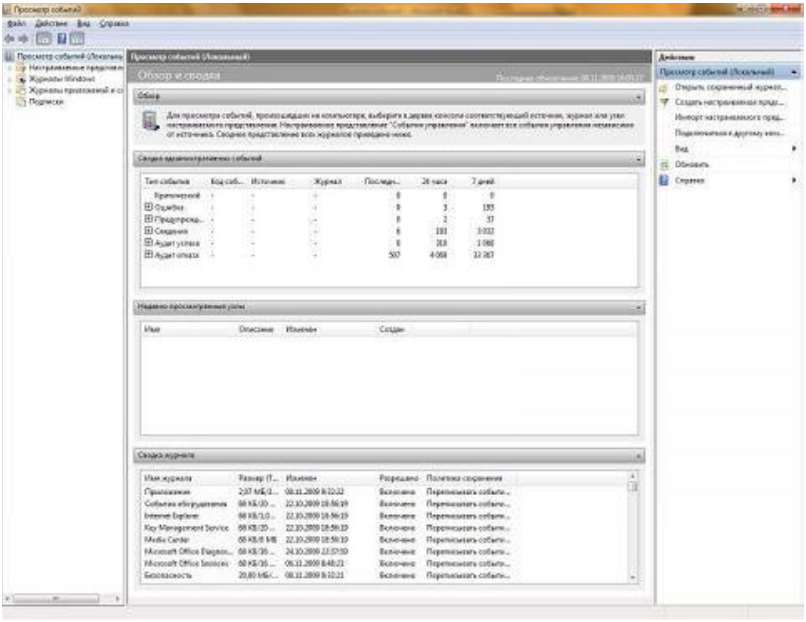

Рис. 2. Интерфейс программы «Просмотр событий»

Приложение «Просмотр событий» можно открыть следующими способами:

— «Пуск» > «Панель управления» > «Администрирование» > «Просмотр событий»;

— «Консоль управления MMC» («Пуск» > ввести “mmc” и нажать “Enter”). При открытии пустой консоли MMC в меню «Консоль» следует выбрать команду «Добавить или удалить оснастку» или воспользоваться комбинацией клавиш Ctrl + M. В диалоге «Добавление и удаление оснасток» нужно выбрать оснастку «Просмотр событий» и нажать «Добавить», «Готово», а после — «ОК»;

— воспользоваться комбинацией клавиш + R для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» ввести eventvwr.msc и нажать «ОК».

В операционных системах Windows 7 и Windosw Vista существуют две категории журналов событий: журналы Windows и журналы приложений и служб (рис. 3).

Журналы Windows используются операционной системой для регистрации общесистемных событий, связанных с работой приложений, системных компонентов, безопасностью и запуском.

Журналы приложений и служб используются приложениями и службами для регистрации событий, связанных с их работой.

Для управления журналами событий можно использовать оснастку «Просмотр событий» или программу командной строки wevtutil, о которой будет рассказано ниже.

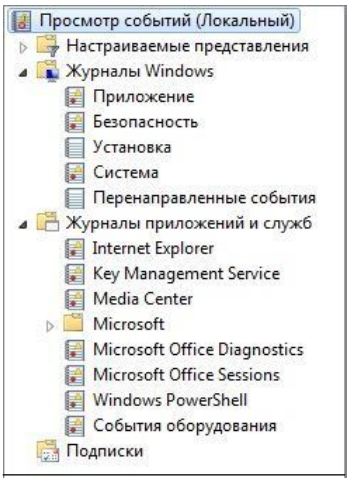

Рис. 3. Журнал событий ОС Windows

Приложение хранит важные события, связанные с конкретным приложением. Например, Exchange Server сохраняет события, относящиеся к пересылке почты, в том числе события информационного хра-

нилища, почтовых ящиков и запущенных служб. По умолчанию помещается в %SystemRoot%\System32\Winevt\Logs\Application.Evtx.

Безопасность хранит события, связанные с безопасностью: вход/выход из системы, использование привилегий и обращение к ресурсам. По умолчанию помещается в %SystemRoot%\System32\Winevt\Logs\Security.Evtx.

Установка. В этот журнал записываются события, возникающие при установке/настройке операционной системы и ее компонентов. По умолчанию размещается в %SystemRoot%\System32\Winevt\Logs\Setup.Evtx.

Система хранит события операционной системы или ее компонентов, например, неудачи при запусках служб или инициализации драйверов, общесистемные сообщения и прочие сообщения, относящиеся к системе в целом. По умолчанию помещается в %SystemRoot%\System32\Winevt\Logs\System.Evtx.

Пересылаемые события. Если настроена пересылка событий, в этот журнал попадают события, пересылаемые с других серверов. По умолчанию помещается в %SystemRoot%\System32\Winevt\Logs\ForwardedEvents.Evtx.

Internet Explorer. В этот журнал записываются события, возникающие при настройке и работе с браузером Internet Explorer. По умолчанию помещается в %SystemRoot%\System32\Winevt\Logs\InternetExplorer.Evtx.

Windows PowerShell. В данном журнале регистрируются события, связанные с использованием оболочки PowerShell. По умолчанию размещается в %SystemRoot%\System32\Winevt\Logs\WindowsPowerShwll.Evtx.

События оборудования. Если настроена регистрация событий оборудования, то в этот журнал записываются события, генерируемые устройствами. По умолчанию помещается в %SystemRoot%\System32\Winevt\Logs\HardwareEvent.Evtx.

В Windows 7 и в Windows Vista инфраструктура, обеспечивающая регистрацию событий, основана на XML. Данные о каждом событии соответствуют XML-схеме, что позволяет получить доступ к XML-коду любого события. Кроме того, можно создавать основанные на XML запросы для получения данных из журналов. Для использования этих новых возможностей не требуются знания об XML. Оснастка «Просмотр событий» предоставляет простой графический интерфейс для доступа к этим возможностям.

Свойства событий

Существует несколько свойств событий оснастки «Просмотр событий», которые подробно описаны ниже:

Источник — программа, зарегистрировавшая событие в журнале. Это может быть как имя программы (например, Exchange Server), так и название компонента системы или большого приложения (например, имя драйвера). Например, Elnkii означает драйвер EtherLink II.

Код события — число, определяющее конкретный тип события. В первой строке описания обычно содержится название типа события. Например, 6005 — идентификатор события, которое происходит при запуске службы ведения журналов событий. Соответственно, в начале описания этого события находится строка «Запущена служба журнала событий». Код события и имя источника записи могут использоваться представителями группы поддержки программного продукта для устранения неполадок.

Уровень — это уровень важности события. В журналах системы и приложений события могут иметь следующие уровни важности:

— *уведомление* обозначает изменение в приложении или компоненте: возникновение информационного события, связанного с успешным действием, создание ресурса или запуск службы;

— *предупреждение* обозначает предупреждение общего характера на неполадку, способную повлиять на службу или привести к более серьезной проблеме, если оставить ее без внимания;

— *ошибка* обозначает, что возникла проблема, которая может повлиять на функции, внешние по отношению к приложению или компоненту, вызвавшим событие;

— *критическая ошибка* обозначает, что произошел сбой, после которого приложение или компонент, инициировавшие событие, не могут восстановиться автоматически;

— *аудит успехов* — успешное выполнение действий, которые вы отслеживаете через аудит, например, использование какой-либо привилегии;

— *аудит отказов* — неудачное выполнение действий, которые вы отслеживаете через аудит, например, ошибка при входе в систему.

Пользователь определяет учетную запись пользователя, от имени которого возникло данное событие. К пользователям относятся особые сущности, например, Local Service, Network Service и Anonymous Logon, а также учетные записи реальных пользователей. Это имя представляет собой идентификатор клиента, если событие фактически было вызвано серверным процессом, или основной идентификатор, если олицетворение не производится. В некоторых случаях запись журнала безопас-

ности содержит оба идентификатора. В этом поле может стоять и N/A (Н/Д), если в данной ситуации учетная запись неприменима. Олицетворение происходит в случаях, когда сервер позволяет одному процессу присвоить атрибуты безопасности другого.

Рабочий код содержит числовое значение, которое определяет операцию либо точку в пределах операции, при выполнении которой возникло данное событие. Например, инициализация или закрытие.

Журнал — имя журнала, в который было записано данное событие.

Категория и задачи определяют категорию события, иногда используемую для последующего описания допустимого действия. У каждого источника событий свои категории. Например, вход/выход, использование привилегий, изменение политики и управление учетной записью.

Ключевые слова — это набор категорий или меток, которые могут использоваться для фильтрации или поиска событий. Например, «Сеть», «Безопасность» или «Ресурс не найден».

Компьютер — идентифицирует имя компьютера, на котором произошло событие. Обычно это имя локального компьютера, но также может быть имя компьютера, переславшего событие, или имя локального компьютера до того, как оно было изменено.

Дата и время — определяет дату и время возникновения данного события в журнале.

ИД процесса представляет идентификационный номер процесса, создавшего данное событие. Компьютерная программа представляет только пассивную совокупность инструкций, в то время как процесс — это непосредственное выполнение этих инструкций.

ИД потока представляет идентификационный номер потока, создавшего данное событие. Процесс, порожденный в операционной системе, может состоять из нескольких потоков, выполняющихся параллельно, т. е. без предписанного порядка во времени. При выполнении некоторых задач такое разделение может достичь более эффективного использования ресурсов вычислительной машины.

ИД процессора представляет идентификационный номер процессора, обработавшего событие.

Код сеанса — идентификационный номер сеанса на сервере терминалов, в котором произошло событие.

Время работы в режиме ядра определяет время, потраченное на выполнение инструкций режима ядра (в единицах времени центрального процессора (далее — ЦП)). Режим ядра имеет неограниченный доступ к системной памяти и внешним устройствам. Ядро системы NT называют гибридным ядром, или макроядром.

Время работы в пользовательском режиме — определяет время, потраченное на выполнение инструкций пользовательского режима (в единицах времени ЦП). Режим пользователя состоит из подсистем, которые передают запросы ввода/вывода соответствующему драйверу режима ядра посредством менеджера ввода-вывода.

Загруженность процессора — время, потраченное на выполнение инструкций пользовательского режима (в тиках ЦП).

Код корреляции определяет действие в процессе, для которого используется событие. Этот код используется для указания простых отношений между событиями. Корреляция — статистическая взаимосвязь двух или нескольких случайных величин (либо величин, которые можно с некоторой допустимой степенью точности считать таковыми). Изменения одной или нескольких из этих величин приводят к систематическому изменению другой (других) величин.

ИД относительной корреляции определяет относительное действие в процессе, для которого используется событие.

Просмотр событий

На скриншоте мы увидим журнал «Приложения», в котором можно узнать сведения о событиях, недавних представлениях и доступных действиях (рис. 4). Чтобы просмотреть события журнала приложений, необходимо выполнить следующие действия:

1) в дереве консоли выбрать «Журналы Windows»;

2) выбрать журнал «Приложения».

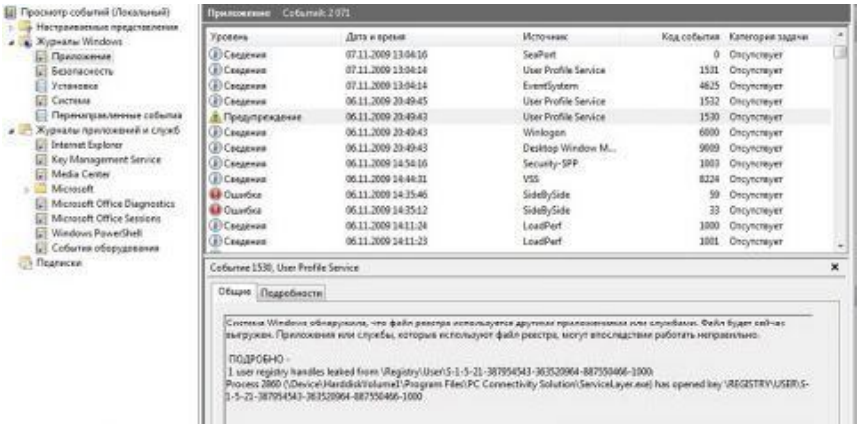

Рис. 4. Интерфейс журнала «Приложения»

При выборе журнала в среднем окне отображаются доступные события, включая дату события, время и источник, уровень события и другие сведения.

Панель *«Область просмотра»* показывает основные данные о событиях на вкладке *«Общие»*, а дополнительные специфические данные — на вкладке *«Подробности»*. Включить и выключить эту панель можно, выбрав меню *«Вид»*, а затем команду *«Область просмотра»*.

Для критических систем рекомендуется хранить журналы за последние несколько месяцев. Для назначения журналам соответствующего размера можно экспортировать журналы в файлы, распложенные в заданной папке. Для сохранения выбранного журнала:

1) в дереве консоли выбрать журнал событий, который нужно сохранить;

2) выбрать команду *«Сохранить события как»* из меню *«Действие»* или из контекстного меню журнала выбрать команду *«Сохранить все события как»*;

3) в появившемся диалоге *«Сохранить как»* выбрать папку для сохранения файла. В поле *«Тип файла»* выбрать желаемый формат файла из доступных: файлы событий — *.evtx, xml-файл — *.xml, текст с разделением табуляции — *.txt, csv с разделением запятыми — *.csv. В поле *«Имя файла»* ввести имя и нажать кнопку *«Сохранить»*;

4) если журнал событий не предназначен для просмотра на другом компьютере, в диалоговом окне *«Отображать сведения»* надо оставить заданный по умолчанию вариант *«Не отображать сведения»*, а если журнал предназначается для просмотра на другом компьютере, то в диалоговом окне *«Отображать сведения»* следует выбрать вариант *«Отображать сведения для следующих языков»* и нажать кнопку *«ОК»* (рис. 5).

Очистка журнала событий

Для очистки выбранного журнала необходимо выполнить следующие действия:

1) в дереве консоли выбрать требуемый журнал событий;

2) очистить журнал одним из следующих способов:

— в меню «Действие» выбрать команду *«Очистить журнал»*;

— на выбранном журнале нажать правой кнопкой для открытия контекстного меню и выбора команды *«Очистить журнал»* (рис. 6).

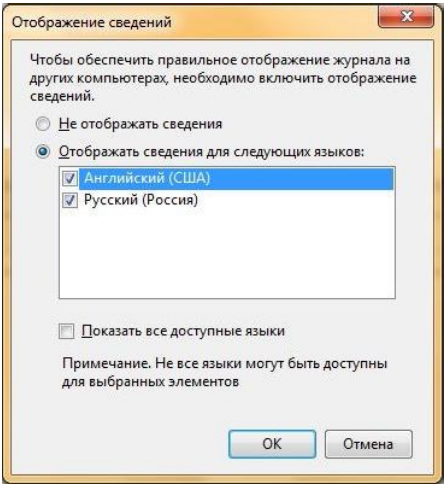

Рис. 5. Диалоговое окно журнала событий

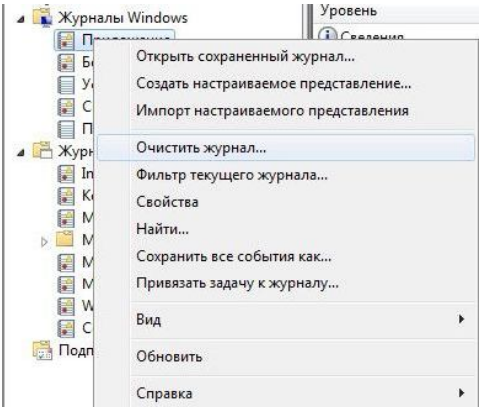

Рис. 6. Очистка журнала событий

3) далее можно очистить журнал либо заархивировать его в том случае, если это не было сделано ранее:

— для очистки без сохранения нажать кнопку *«Очистить»*;

— для очистки журнала событий после его сохранения нажать кнопку *«Сохранить и очистить»*.

Установка максимального размера журнала

Журналы событий хранятся в виде файлов в папке %SystemRoot%\System32\Winevt\Logs\. По умолчанию максимальный размер этих файлов ограничен, но его можно изменить следующим способом:

1) в дереве консоли выбрать журнал событий, для которого следует изменить размер;

2) выбрать команду *«Свойства»* из меню *«Действие»* или из контекстного меню выбранного журнала;

3) в поле *«Максимальный размер журнала (КБ)»* установить требуемое значение при помощи счетчика или вручную (без использования счетчика) (рис. 7).

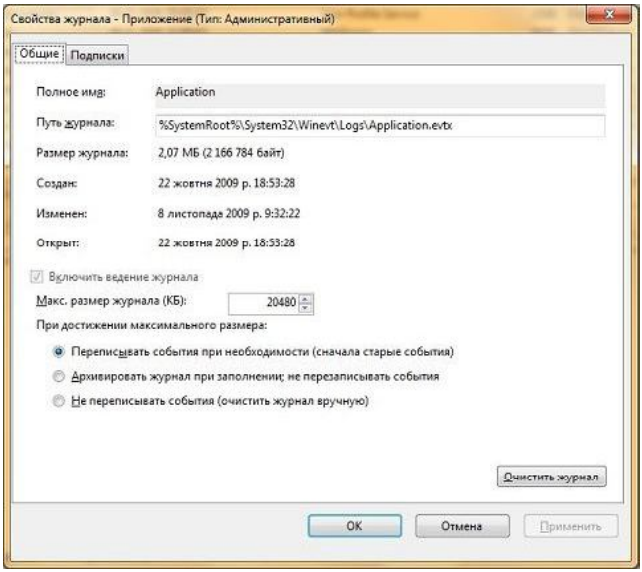

Рис. 7. Диалоговое окно «Свойства журнала событий»

В этом случае значение будет округлено до ближайшего числа, кратного 64 Кб, так как размер файла журнала должен быть кратен 64 Кб и не может быть меньше 1024 Кб.

События сохраняются в файле журнала, размер которого может увеличиваться только до заданного максимального значения. После достижения файлом максимального размера обработка поступающих событий будет определяться политикой хранения журналов. Доступны следующие политики сохранения журнала:

1. ***Переписывать события при необходимости (сначала старые файлы).*** В этом случае новые записи продолжают заноситься в журнал

после его заполнения, каждое новое событие заменяет в журнале наиболее старое.

2. ***Архивировать журнал при заполнении, не переписывать события.*** Файл журнала автоматически архивируется при необходимости. Перезапись устаревших событий не выполняется.

3. ***Не переписывать события (очистить журнал вручную).*** Журнал очищается вручную, а не автоматически.

Чтобы выбрать нужную политику сохранения журналов, необходимо выполнить следующие действия:

1) в дереве консоли выбрать журнал событий, для которого следует изменить размер;

2) выбрать команду *«Свойства»* из меню *«Действие»* или из контекстного меню выбранного журнала;

3) на вкладке *«Общие»* в разделе *«При достижении максимального размера»* выбрать требуемый параметр, нажать кнопку *«ОК»* (рис. 8).

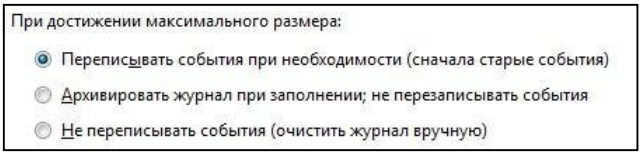

Рис. 8. Политика сохранения журнала

Активация аналитического и отладочного журнала

Аналитический и отладочный журналы по умолчанию неактивны. После активации они быстро заполняются большим количеством событий. По этой причине желательно активировать указанные журналы на ограниченное время, чтобы собрать необходимые для поиска и устранения неполадок данные, а затем их снова отключить. Активацию журналов можно выполнить следующим образом:

1) в дереве консоли выбрать аналитический или отладочный журнал для активации;

2) выбрать команду *«Свойства»* из меню *«Действие»* или из контекстного меню выбранного аналитического или отладочного журнала;

3) на вкладке *«Общие»* установите флажок на опции *«Включить ведение журнала»*.

Открытие и закрытие сохраненного журнала

При помощи оснастки «Просмотр событий» можно открывать и просматривать сохраненные ранее журналы (рис. 9). Одновремен-

но можно открыть несколько сохраненных журналов и обращаться к ним в любое время в дереве консоли. Журнал, открытый в «Просмотре событий», может быть закрыт без удаления содержащихся в нем сведений.

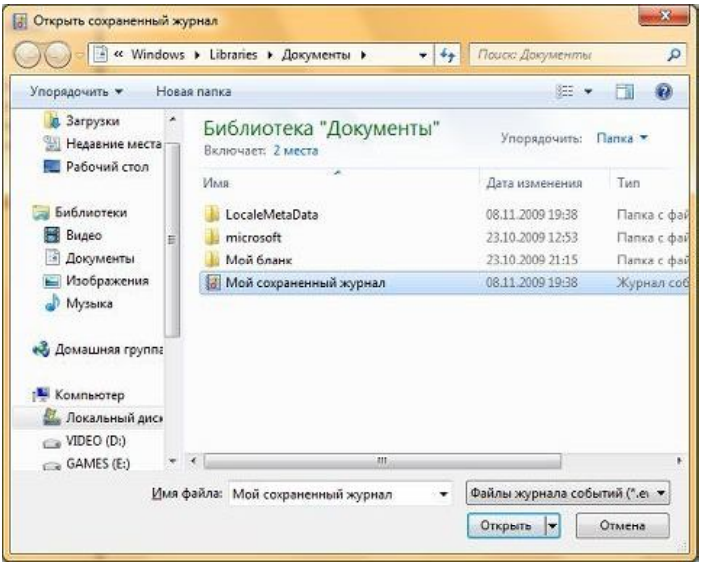

Рис. 9. Открытие сохраненного журнала

Для открытия сохраненного журнала необходимо выполнить следующие действия:

1) выбрать команду *«Открыть сохраненный журнал»* в меню *«Действие»* или из контекстного меню в дереве консоли;

2) в диалоговом окне *«Открыть сохраненный журнал»*, передвигаясь по дереву каталогов, открыть папку, содержащую нужный файл. По умолчанию в диалоговом окне будут выведены все файлы журналов событий. При открытии можно выбрать и тип файлов, которые нужно отображать в диалоге открытия. Доступные типы файлов: файлы журнала событий (*.evtx, *.evt, *.etl), файлы событий (*.evtx), старые файлы событий (*.evt) или файлы журнала трассировки (*.etl). Если нужный файл журнала будет найден, выделите его, щелкнув по нему левой кнопкой мыши, что поместит его имя в строку для ввода имени файла, затем следует нажать кнопку *«Открыть»*;

3) в диалоге *«Открыть сохраненный журнал»* в поле *«Имя»* ввести новое имя, которое будет использоваться для журнала в дереве консоли. Оно используется только для представления журнала в дереве консоли, имя файла журнала при этом не изменяется. Можно использовать существующее имя файла журнала. В поле «Описание» следует ввести описание журнала. Оно будет отображаться в центральной области при выделении родительской папки журнала в дереве консоли;

4) для создания папки сохранения надо нажать на кнопку «Создать папку». В поле *«Имя»* ввести имя папки, в которой будет находиться открытый журнал, нажать *«ОК»* (рис. 10). Если родительская папка не выбрана, новая папка будет расположена в папке *«Сохраненные журналы»*.

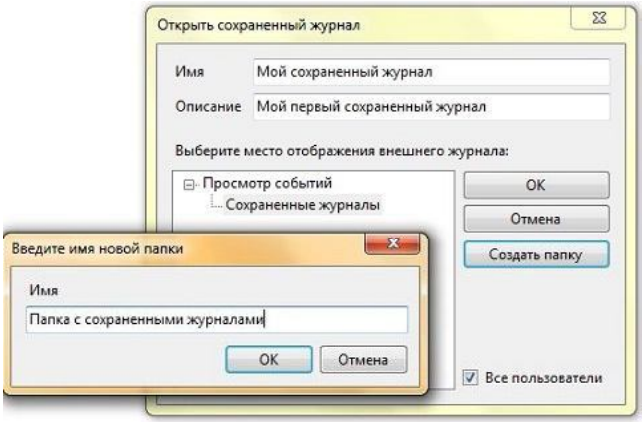

Рис. 10. Создание папки сохранения

5) чтобы открытый журнал событий стал недоступным для других пользователей компьютера, можно снять флажок *«Все пользователи»*. Если этот флажок останется активным, открытый журнал будет доступен всем пользователям, но для его удаления из дерева консоли потребуются права администратора;

6) для открытия журнала нажать *«ОК»*.

Для удаления открытого журнала из дерева событий (рис. 11):

1) в дереве консоли выбрать журнал, который следует удалить;

2) выбрать команду *«Удалить»* из меню *«Действие»* или из контекстного меню выбранного журнала;

3) в диалоге *«Просмотр событий»* нажать *«Да»*.

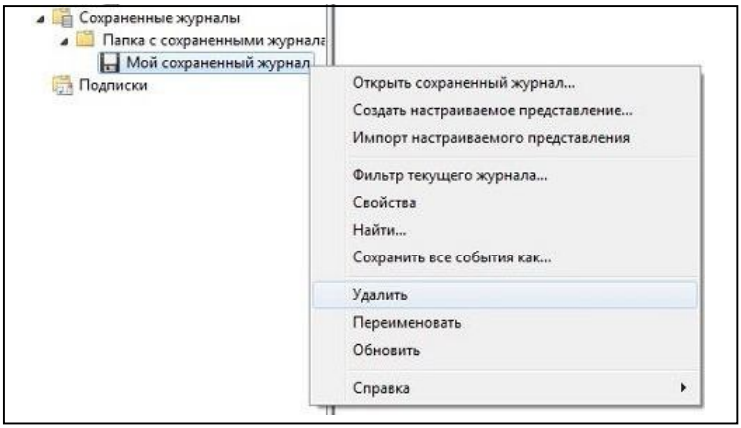

Рис. 11. Удаление открытого журнала из дерева событий

§ 3. Реестр Windows

Реестр — иерархически построенная база данных в составе операционной системы Windows, содержащая конфигурационные сведения. Вся информация реестра разбита на несколько файлов. Реестры разных версий Windows частично отличаются. В Windows 95/98 реестр содержится в двух файлах **SYSTEM.DAT** и **USER.DAT**, находящихся в каталоге Windows. В Windows Me был добавлен файл **CLASSES.DAT**. В Windows XP реестр хранится во многих файлах. Основная часть хранится в файлах **sam**, **security**, **software**, **system**, **default** (все файлы без расширения). По замыслу Microsoft, он должен был полностью заменить файлы ini, которые были оставлены только для совместимости со старыми программами, ориентированными на более ранние версии операционной системы Windows.

Обозначения:

HKLM = HKEY_LOCAL_MACHINE;

HKCU = HKEY_CURRENT_USER;

HKCR = HKEY_CLASSES_ROOT.

Разделы реестра обозначаются жирным шрифтом:

HKLM\System\CurrentControlSet\Control\Lsa.

Все настройки даны для текущего пользователя (раздел HKEY_CURRENT_USER). Если существует аналогичная запись в HKEY_LOCAL_MACHINE (для всей системы), то ***HKCU*** выделяется ***жирным курсивом***.

В реестре хранятся данные, которые необходимы для правильного функционирования Windows. К ним относятся профили пользователей, сведения об установленном программном обеспечении и типах документов, которые могут быть созданы каждой программой, информация о свойствах папок и значках приложений, а также об установленном оборудовании и используемых портах.

Редактирование реестра. Основным средством для просмотра и редактирования записей реестра служит специализированная утилита «Редактор реестра». Для ее запуска выберите *Пуск > Выполнить* и введите команду *regedit*. Откроется окно программы, где слева отображается дерево реестра, аналогичное отображению структуры диска в Проводнике, а справа выводятся ключи, содержащиеся в выбранном (активном) разделе. С помощью редактора можно редактировать значения, импортировать или экспортировать реестр, осуществлять поиск.

Существует пять разделов реестра верхнего уровня. Переход между разделами реестра в окне редактора реестра происходит так же, как и переход между папками в проводнике Windows.

Реестр 64-разрядных версий Windows XP и Windows Server 2003 подразделяется на 32- и 64-разрядные разделы. Большинство 32-разрядных разделов имеют те же имена, что и их аналоги в 64-разрядном разделе, и наоборот. По умолчанию редактор реестра 64-разрядных версий Windows XP и Windows Server 2003 отображает 32-разрядные разделы в следующем узле: **HKEY_LOCAL_MACHINE\Software\WOW6432**

В Windows XP и Windows Server 2003 имеется программа **regedt32.exe**, которая оставлена в целях совместимости. На самом деле она просто запускает программу **regedit.exe**.

Надстройки реестра Windows

Удаление списка часто используемых программ. Для удаления списка часто используемых программ через кнопку **Пуск** надо открыть раздел **HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer** и создать параметр NoStartMenuMFUprogramsList типа **DWORD** со значением, равным 1.

Запрет на попадание приложения в список часто используемых программ. Можно не удалять список часто используемых программ, а запретить отдельным программам попадать в этот список. Для этого необходимо открыть раздел **HKCR\Applications\Имя_Программы.exe** и создать пустой строковый параметр NoStartPage.

Удаление имени пользователя. Для удаления имени пользователя в кнопке **Пуск** надо открыть раздел **HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer** и создать параметр NoUser NameInStartMenu типа **DWORD** со значением, равным 1.

Удаление вышеприведенных параметров или установка в 0 возвращает прежнее поведение.

Папки. Существует возможность скрывать папки и файлы из верхней части меню кнопки **Пуск**, которые были скопированы из других мест (папки при этом не удаляются). В разделе ***HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer*** следует создать параметр типа **DWORD** NoStartMenuSubFolders со значением 1.

Программы. Для сокрытия приложения из выпадающего меню кнопки **Пуск** из папки "C:\Documents and Settings\All Users\Главное меню\Программы" необходимо открыть раздел **HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer** и создать параметр типа **DWORD** NoCommonGroups со значением 1.

Управление количеством запоминаемых документов

Windows помнит список из 15 последних открытых документов, доступ к которому можно получить через **Пуск** > **Документы**. Для изменения этого значения надо открыть раздел ***HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer*** и создать параметр MaxRecentDocs типа ***DWORD*** со значением от 0x0–0xFFFFFFFF (0xF = 15 документам).

Автоматическое очищение списка недавно открытых документов при выключении компьютера: необходимо добавить ключ ClearRecentDocsOnExit типа **DWORD** со значением 1 в разделе ***HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer***

Не запоминать открываемые документы — надо добавить ключ NoRecentDocsHistory типа **DWORD** со значением 1 в разделе ***HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer***

Очистка истории ранее вводимых слов — удалить подраздел ACMru в разделе ***HKCU\Software\Microsoft\Search Assistant.*** Для постоянной очистки данного раздела можно поместить в автозагрузку команду >regedit /s Clear.reg, а в папке Windows создать файл Clear.reg с содержанием: REGEDIT4 [-HKEY_CURRENT_USER\Software\Microsoft\Search Assistant\ACMru].

После этого история поиска файлов будет очищаться автоматически при запуске системы.

Удаление параметра или установка в 0 возвращает пункт в меню.

Удаление пункта Выполнить из меню кнопки Пуск — открыть раздел ***HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer*** и создать параметр типа **DWORD** NoRun со значением 1.

Очистка списка недавно использованных команд

Команда **Выполнить** содержит список недавно использованных команд (MRU list). Этот список содержится в разделе ***HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU***.

Параметр MRUList содержит строку, определяющую порядок, в котором остальные записи будут появляться в списке. Например, запись "bca" говорит о том, что первым элементом в списке **Открыть** будет команда с именем **b**, потом **c**, затем **a**.

Сами команды хранятся как строки с оканчивающимися символами **\1** в параметрах a, b, c, d и т. д. Всего допускается 26 записей.

Для очистки списка нужно заменить параметры MRUList и все команды пустой строкой (« ») либо отредактировать самостоятельно.

Завершение работы

Выключить компьютер можно двумя способами:

— используя команду **Выключение** в меню кнопки **Пуск**;

— открывая окно **Диспетчер задач Windows** нажатием кнопок Ctrl+Alt+Del, выбирая пункт в меню **Завершение работы** > **Выключение.**

Windows позволяет запретить выключение этими способами для текущего пользователя. Для этого откройте раздел ***HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer*** и создайте параметр типа **DWORD** NoClose со значением 1. Сразу после изменения в реестре станут недоступны несколько пунктов в меню **Выключение** диалогового окна **Диспетчер задач Windows**. После перезагрузки пункт **Выключение** исчезнет из меню кнопки **Пуск**. Это относится только к стандартным средствам Windows. Специальные программы или утилиты по-прежнему могут выключать компьютер.

Удаление значка Корзины с Рабочего стола. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace** необходимо удалить подраздел {645FF040-5081-101B-9F08-00AA002F954E}.

Связанные документы

В последних версиях Windows появилось понятие сопоставленных файлов. Например, если вы собираетесь переместить или удалить html-документ, то будут перемещены или удалены и сопоставленные с

этим документом файлы, которые содержатся в папке «Имя документа.files». Если вы хотите отключить подобное поведение, то создайте параметр **DWORD** NoFileFolderConnection со значением 1 в разделе **HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer**.

Диски

Сокрытие значков дисков в окне Мой компьютер и Проводник. В разделе ***HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer*** создайте параметр NoDrives типа **DWORD** с требуемым значением. Эти значки будут скрыты и в стандартных окнах Открытия и Сохранения файлов. Пользователь по-прежнему имеет доступ к этим дискам (через команду *выполнить* или печатая вручную адрес в адресной строке Проводника).

Данный параметр является набором битовых флагов. Бит соответствует одному из 26 возможных имен дисков. Каждому диску присваиваются значения (hex): A — 1; B — 2; C — 4 и т. д. Чтобы скрыть нужные вам диски, следует сложить эти биты. Сложность заключается в переводе двоичного значения в шестнадцатиричное. Здесь приводится небольшой список возможных значений:

0x03FFFFFF — скрывает все значки;
0x3 — скрывает только диски A и B;
0x4 — скрывает только диск C;
0x8 — скрывает только диск D;
0x7 — скрывает только диски A, B и C;
0xF — скрывает только диски A, B, C и D;
0x0 — видны все диски.

Запрет на доступ к содержимому выбранных дисков. Можно не скрывать сами значки дисков, но запретить пользователю доступ к файлам заданных дисков через Проводник, Мой компьютер, Выполнить или команду Dir. Откройте реестр и создайте параметр NoViewOnDrive типа **DWORD** в разделе ***HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer,*** содержащий битовую маску для дисков. Например, диск A имеет бит 1, диск C — 4, диск D — 8. Чтобы скрыть диски A и D, нужно сложить их значения 1 (A) + 8 (D) и установить значение 9.

Список всех дисков:

A: 1, B: 2, C: 4, D: 8, E: 16, F: 32, G: 64, H: 128, I: 256, J: 512, K: 1024, L: 2048, M: 4096, N: 8192, O: 16384, P: 32768, Q: 65536, R: 131072, S: 262144, T: 524288, U: 1048576, V: 2097152, W: 4194304, X: 8388608, Y: 16777216, Z: 33554432. Все диски: 67108863.

Временные файлы Интернета. На вкладке **Общие** можно отключить все кнопки, относящиеся к рамке **Временные файлы Интернета** (Удалить Cookie... Удалить файлы... Параметры...). Для этого присвойте параметру Settings значение 1.

Журнал. Для блокировки рамки **Журнал** присвойте параметру History значение 1.

Автозагрузка. Существует несколько способов прописать программу в автозагрузку. Самый простой — скопировать программу или ярлык в папку Автозагрузка. Есть другой способ — через реестр. Им часто пользуются вредоносные программы. Открыть раздел ***HKLM\Software\Microsoft\Windows\CurrentVersion***, найти подразделы Run, RunOnce. В них есть строковые ключи (некоторые разделы пустые), отвечающие за запуск программ. Название ключа может быть произвольным, а в качестве значения указывается запускаемая программа (если надо, то с параметрами). Обратите внимание на разделы, в названии которых присутствует “Once”. В них прописываются программы, запуск которых надо произвести всего один раз. Например, при установке новых программ некоторые из них прописывают туда ключи, указывающие на какие-нибудь настроечные модули, которые запускаются сразу после перезагрузки компьютера. Такие ключи после своего запуска автоматически удаляются.

В разделе ***HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion*** есть только два подраздела, отвечающие за автозагрузку: Run и Runonce. Изначально они пустые, так что все записи сделаны другими программами.

Списки последних открытых и сохраненных файлов в стандартных окнах открытия и сохранения файлов. При использовании стандартных диалоговых окон Windows сохраняет список последних открытых и сохраненных файлов в реестре. Данный список хранится по адресу ***HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32***.

Запрещение/Разрешение запуска программ

Запрещение запуска программ. Windows позволяет ограничить доступ к программам, кроме разрешенных в специальном списке. Для ограничения запускаемых программ в разделе ***HKCU\SOFTWARE\Microsoft\Windows\CurrentVerson\Policies\Explorer*** необходимо создать ключ RestrictRun типа DWORD со значением 0x00000001. Затем — подраздел с аналогичным именем **RestrictRun** и в нем перечислить список

разрешенных к запуску программ для текущего пользователя. Записи в этом подразделе нумеруются начиная с 1 и содержат строки с путем (необязательно) и именем приложения. Файлы должны быть с расширением. Например, Word.exe, Excel.exe.

Стоит указать и файл Regedit.exe, иначе не получится запустить редактор реестра. Для сброса ограничения на запуск программ надо установить значение ключа **RestrictRun** в 0.

Разрешение запуска приложения, кроме указанных в списке

Можно решить обратную задачу и указать список запрещенных к запуску приложений. В разделе ***HKCU\SOFTWARE\Microsoft\ Windows\ CurrentVerson\Policies\Explorer*** надо создать ключ DisallowRun типа **DWORD** со значением 1. Затем — подраздел с этим же именем **DisallowRun**, и в нем указать список запрещенных программ в виде строковых параметров. Записи в этом подразделе нумеруются начиная с 1, содержат строки с путем (необязательно) и именем приложения. Файлы должны быть с расширением. Например, Word.exe, Excel.exe:

«1» — “calc.exe”;

«2» — “thebat.exe”;

«3» — “hl.exe”.

Эта настройка действует на программы, запускающие процесс от Windows Explorer, но не защищает от запуска данных программ при помощи Диспетчера задач (Task Manager), который запускается системным процессом или другими процессами. Эти программы можно запустить через командную строку Cmd.exe.

Запрет на запуск диспетчера задач Windows. В разделе ***HKCU\ Software\Microsoft\Windows\CurrentVersion\Policies\System*** необходимо установить значение параметра типа **DWORD** DisableTaskMgr, равное 1.

Пароли и безопасность. Рассматриваемые настройки хранятся в ветви ***HKLM*\SOFTWARE\Microsoft\Windows\CurrentVersion\ Policies\Network**.

Все ключи имеют тип **DWORD**, если это не оговорено отдельно; значение ключа, равное 1, включает данную опцию, 0 — выключает (если это не оговорено отдельно).

Отмена кэширования пароля. Данная настройка помогает избавиться от проблемы «утаскивания» и дальнейшего взлома ваших сетевых и интернет-паролей. Эти пароли хранятся в файле с расширением PWL. Отключение кэша запрещает запись паролей в этот файл. Следует использовать параметр типа DisablePwdCaching со значением 1.

Очистка файла подкачки. Файл подкачки *pagefile.sys* находится в корне каждого (или только системного) диска. Там могут оставаться пароли к различным ресурсам и прочая конфиденциальная информация. Для очистки данного файла после завершения работы установите параметр типа **DWORD** ClearPageFileAtShutdown со значением 1 в разделе ***HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management***.

USB. Существует способ запретить использование USB-накопителей в Windows XP. Откройте раздел ***HKLM\SYSTEM\CurrentControlSet\Services\UsbStor*** и установите значение параметра Start, равное 4. USB-диски после этого работать перестанут.

Установка способа доступа к расширенным ресурсам компьютера из сети (Windows NT/2000/XP). Раздел — **HKLM\System\CurrentControlSet\Control\Lsa.** Параметр типа **DWORD** RestrictAnonymous. Значение, равное 1, запрещает анонимным пользователям удаленно просматривать учетные записи и расширенные ресурсы. Значение, равное 2, отказывает любой неявный доступ к системе (в сетевом окружении компьютер не будет виден, однако доступ к нему можно будет получить, обратившись к нему по его IP).

§ 4. Данные о USB-устройствах в реестре Windows

При подключении неизвестного флеш-накопителя Windows начинает процесс установки нового оборудования для найденного USB-устройства. Установка занимает некоторое время, после чего флешка определяется как внешний USB-накопитель и становится видна в проводнике. При повторном подключении флеш-накопителя к компьютеру она корректно распознается системой и сразу появляется в корневом каталоге проводника «Мой компьютер».

Вся информация о любых USB-носителях, когда-либо подключаемых к компьютеру, хранится в системном реестре. Если к компьютеру подключается много флеш-накопителей разных моделей и производителей, то со временем в реестре накапливается лишняя информация. В результате процесс определения и подключения нового устройства начинает занимать значительное время и тормозит систему.

Чтение и чистку реестра надо производить с помощью системной программы Regedit (рис. 12). Запускается она так: *Пуск > Выполнить> Regedit*.

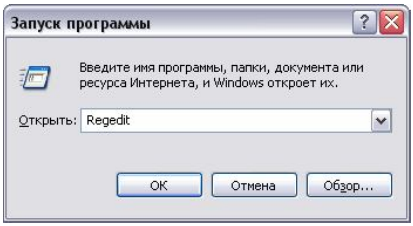

Рис. 12. Запуск программы *Regedit*

Внимание! Эти разделы содержат информацию и о жестких дисках, установленных на компьютере. Не удаляйте эту информацию!

Разделы реестра, которые хранят информацию о любых накопителях, подключавшихся ранее и используемых в настоящее время на компьютере (рис. 13):

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b};

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b};

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}.

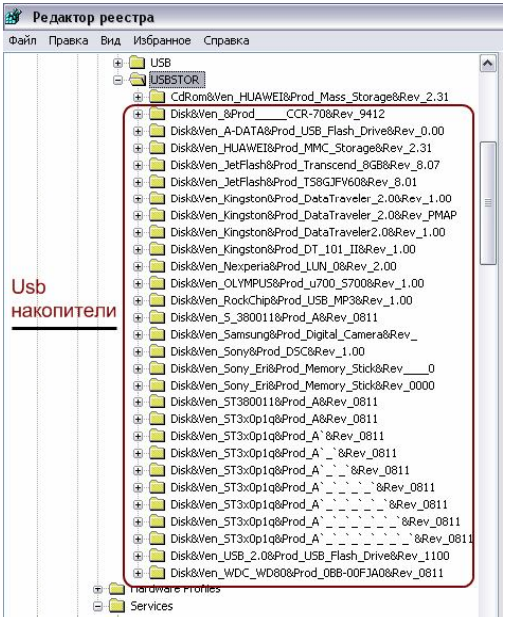

Рис. 13. Редактор реестра

Разделы реестра, хранящие данные о любом USB-накопителе, когда-либо подключаемом к ПК, — это флешки, внешние хард-диски, а также фотоаппараты, телефоны, флеш-плееры и другие устройства, которые при подключении к ПК были распознаны как внешний USB-накопитель:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR;

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR;

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Enum\USBSTOR.

Программа для очистки реестра USBDeview

Программа USBDeview (http://soft-arhiv.com/load/3-1-0-475) показывает всю информацию о ранее подключаемых USB-устройствах, включая дату первого и последнего использования, имеет большое количество настроек, русскоязычное меню, удаляет любые данные из реестра, даже в WIN 7 64-bit (рис. 14).

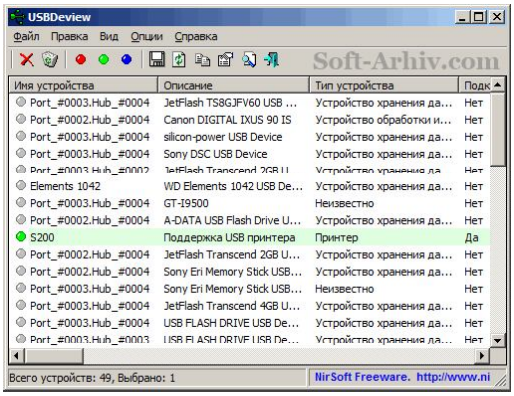

Рис. 14. Интерфейс программы *USBDeview*

Иногда, даже с установленными правами на полный доступ, удалить указанные ключи не получается. Необходим запуск редактора реестра с правами системы. Для этого нужно запустить ее через «Планировщик заданий». Убедитесь, что эта служба включена:

Панель управления > администрирование > службы > Планировщик заданий.

Если все в порядке, то составляем BAT-файл следующего содержания: **at 21:01 /interactive regedit.exe**.

21:01 — это время запуска задачи. Если системные часы показывают время 20:59, то редактор реестра (regedit.exe) будет запущен в 21:01, через две минуты (рис. 15).

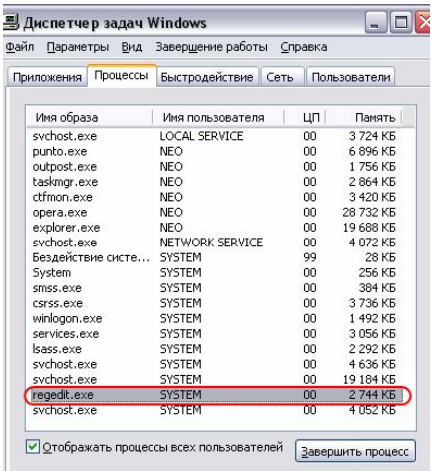

Рис. 15. Диспетчер задач с запущенным редактором реестра (regedit.exe)

После этого запускаем BAT-файл. В 21:01 запускается редактор реестра под системными правами, после чего можно править в реестре любые данные. Для контроля подробного отчета подключения устройств по USB: дата, время, пользователь, данные, скопированные с компьютера или на компьютер, запущенные с USB-носителя файлы и т. д., можно воспользоваться программой USBLogView[1].

§ 5. Механизмы логирования браузеров

Разработчики современных браузеров, с одной стороны, стремятся усовершенствовать свои изобретения и сделать работу пользователя более комфортной, сохраняя пароли и запоминая истории посещения страниц (табл. 5). С другой стороны, подвергают пользователей риску, сохраняя конфиденциальные данные в своих служебных файлах.

Средством анализа может служить программа *Historian*, способная проводить подробный анализ служебных файлов браузера (cookies, список загружаемых файлов, история открываемых страниц). Программа позволяет работать с данными от популярных браузеров Google Chrome, Opera, Firefox, Internet Explorer. Данные, проанализированные с помо-

[1] URL: http://www.nirsoft.net/utils/usb_log_view.html (дата обращения: 10.11.2015).

щью программы *Historian*, позволяют получить подробный отчет о действиях и предпочтениях пользователей, а в некоторых случаях — восстановить сеанс и получить доступ к закрытому аккаунту. Скачать программу можно с официального сайта разработчика[2]. Далее необходимо извлечь архив и запустить exe-файл.

Таблица 5. **Места хранения историй браузеров**

Браузер	Путь сохранения
Google Chrome	C:\Documents and Settings\<Имя пользователя>\Local Settings\Application Data\Google\Chrome\User Data\ Default
Opera	C:\Documents and Settings\<Имя пользователя>\Application Data\Opera\ Opera
Firefox	C:\Documents and Settings\<Имя пользователя>\Application Data\Mozila\ Firefox\Profiles\<Выбираем профиль>
Internet Explorer	C:\Documents and Settings\<Имя пользователя>\Cookies

Открытие файла производится через пункт меню File, после чего автоматически определяется версия браузера и хранящиеся данные в файле. Формат файла отчета и путь можно указать через меню File > Select output file… (рекомендуется txt-формат) (рис. 16).

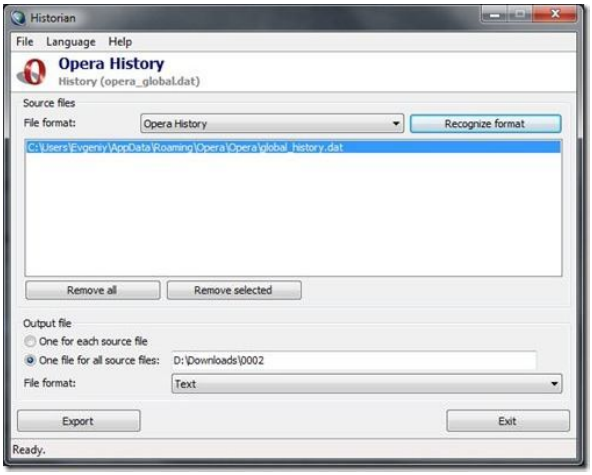

Рис. 16. Интерфейс программы *Historian*

[2] URL: http://depositfiles.com/files/s807hgfbq (дата обращения: 11.11.2015).

После выбора “Export” будет создан файл-отчет. Он содержит достаточно обширные сведения о действиях пользователя в Интернете (рис. 17). Наиболее полную картину можно получить после анализа всех возможных файлов.

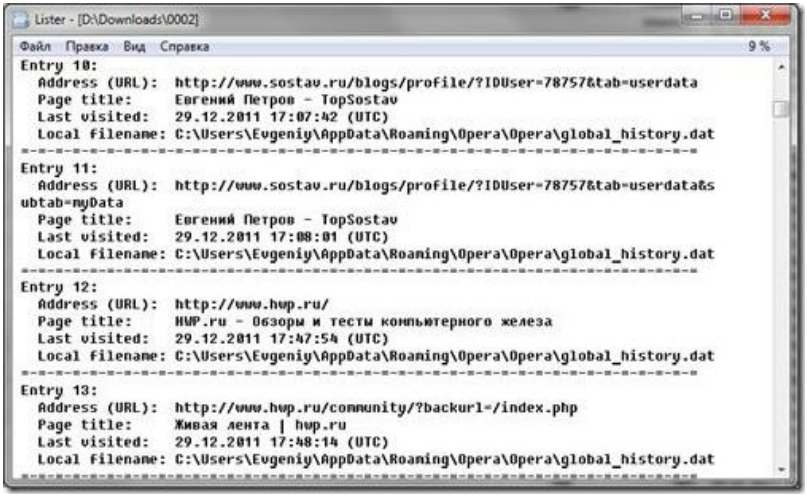

Рис 17. Файл-отчет программы *Historian*

ГЛАВА IV. ИНТЕРНЕТ

§ 1. Структура сети

Стек* протоколов TCP/IP. IP-адресация

В настоящее время стек TCP/IP широко используется как в глобальных, так и в локальных сетях. Этот стек имеет иерархическую структуру, в которой определено четыре уровня:

1) прикладной уровень (FTP, Telnet, HTTP, SMTP, SNMP, TFTP);

2) транспортный уровень (TCP, UDP);

3) сетевой уровень (IP, ICMP, RIP, OSPF);

4) уровень сетевых интерфейсов.

Прикладной уровень стека TCP/IP соответствует трем верхним уровням модели OSI: прикладному, представления и сеансовому. Он объединяет сервисы, предоставляемые системой пользовательским приложениям. За долгие годы применения в сетях различных стран и организаций стек TCP/IP накопил большое количество протоколов и служб прикладного уровня. К ним относятся такие распространенные протоколы, как протокол передачи файлов (File Transfer Protocol, FTP), протокол эмуляции терминала telnet, простой протокол передачи почты (Simple Mail Transfer Protocol, SMTP), протокол передачи гипертекста (Hypertext Transfer Protocol, HTTP) и многие другие. Протоколы прикладного уровня развертываются на хостах.

Транспортный уровень стека TCP/IP может предоставлять вышележащему уровню два типа сервиса:

— гарантированную доставку обеспечивает протокол управления передачей (Transmission Control Protocol, TCP);

— доставку по возможности, или с максимальными усилиями, обеспечивает протокол пользовательских дейтаграмм (User Datagram Protocol, UDP).

Чтобы обеспечить надежную доставку данных, протокол TCP предусматривает установление логического соединения, что позволяет ему

---

* Под стеком в информатике понимается динамическая структура данных с последовательным доступом в порядке, обратном порядку добавления их в стек (принцип LIFO (LAST in Fist out) — последним пришел, первым ушел).

нумеровать пакеты, подтверждать их прием квитанциями, а в случае потери — организовать повторные передачи, распознать и уничтожить дубликаты, а также доставлять прикладному уровню пакеты в том порядке, в котором они были отправлены. Благодаря этому протоколу объекты на хосте-отправителе и хосте-получателе могут поддерживать обмен данными в дуплексном режиме.

В Интернете (и в стеке протоколов TCP/IP) конечный узел традиционно называют *хостом,* а маршрутизатор — *шлюзом.* Далее мы будем использовать пары «конечный узел — хост» и «маршрутизатор — шлюз» как синонимы, чтобы отдать дань уважения традиционной терминологии Интернета и в то же время не отказываться от современных терминов.

Протокол TCP дает возможность без ошибок доставить сформированный на одном из компьютеров поток байтов на любой другой компьютер, входящий в составную сеть. Второй протокол этого уровня, UDP, является простейшим дейтаграммным протоколом, который используется, когда задача надежного обмена данными не ставится либо решается средствами более высокого уровня — прикладным уровнем или пользовательскими приложениями.

В функции протоколов TCP и UDP входит исполнение роли связующего звена между прикладным и сетевым уровнями, прилегающими к транспортному. От прикладного протокола транспортный уровень принимает задание на передачу данных с тем или иным качеством прикладному уровню-получателю. Нижележащий сетевой уровень протоколы TCP и UDP рассматривают как инструмент (не очень надежный, но способный перемещать пакет в свободном и рискованном путешествии по составной сети).

Программные модули, реализующие протоколы TCP и UDP, подобно модулям протоколов прикладного уровня, устанавливаются на хостах.

Сетевой уровень, называемый ***уровнем Интернета***, является стержнем всей архитектуры TCP/IP. Именно этот уровень, функции которого соответствуют сетевому уровню модели OSI, обеспечивает перемещение пакетов в пределах составной сети, образованной объединением нескольких подсетей. Протоколы сетевого уровня поддерживают интерфейс с вышележащим транспортным уровнем, получая от него запросы на передачу данных по составной сети, а также с нижележащим уровнем сетевых интерфейсов.

Основным протоколом сетевого уровня является межсетевой протокол (Internet Protocol, IP). В его задачу входит продвижение пакета меж-

ду сетями — от одного маршрутизатора к другому, пока пакет не попадет в сеть назначения. В отличие от протоколов прикладного и транспортного уровней, протокол IP развертывается не только на хостах, но и на всех маршрутизаторах (шлюзах). Протокол IP — это дейтаграммный протокол, работающий без установления соединений по принципу доставки с максимальными усилиями. Такой тип сетевого сервиса называют ненадежным.

К сетевому уровню TCP/IP часто относят протоколы, выполняющие вспомогательные функции по отношению к IP. Это, прежде всего, протоколы маршрутизации RIP и OSPF, предназначенные для изучения топологии сети, определения маршрутов и составления таблиц маршрутизации, на основании которых протокол IP перемещает пакеты в нужном направлении. По этой же причине к сетевому уровню может быть отнесен протокол межсетевых управляющих сообщений (Internet Control Message Protocol, ICMP), предназначенный для передачи маршрутизатором источнику сведений об ошибках, возникших при передаче пакета, и некоторые другие протоколы.

Идеологическим отличием архитектуры стека TCP/IP от многоуровневой архитектуры других стеков является интерпретация функций самого нижнего уровня — ***уровня сетевых интерфейсов***.

У нижнего уровня стека TCP/IP задача существенно проще — он отвечает только за организацию взаимодействия с подсетями разных технологий, входящими в составную сеть.

TCP/IP рассматривает любую подсеть, входящую в составную, как средство транспортировки пакетов между двумя соседними маршрутизаторами.

Задачу организации интерфейса между технологией TCP/IP и любой другой технологией промежуточной сети упрощенно можно свести к двум задачам:

— упаковка (инкапсуляция) IP-пакета в единицу передаваемых данных промежуточной сети;

— преобразование сетевых адресов в адреса технологии данной промежуточной сети.

Такой гибкий подход упрощает решение проблемы расширения набора поддерживаемых технологий.

Потоком данных, информационным потоком или ***потоком***, называют данные, поступающие от приложений на вход протоколов транспортного уровня — TCP и UDP.

Протокол TCP нарезает из потока данных ***сегменты.***

Единицу данных протокола UDP часто называют ***дейтаграммой*** или ***датаграммой***. Дейтаграмма — это общее название для единиц данных, которыми оперируют протоколы без установления соединений. К таким протоколам относится и протокол IP, поэтому его единицу данных иногда тоже называют дейтаграммой, хотя часто используется и другой термин — ***пакет***.

В стеке TCP/IP единицы данных любых технологий, в которые упаковываются IP-пакеты для их последующей передачи через сети составной сети, принято называть ***кадрами*** или ***фреймами***. При этом не имеет значения, какое название используется для этой единицы данных в технологии составляющей сети. Для TCP/IP фреймом является и кадр Ethernet, и ячейка ATM, и пакет X.25 в тех случаях, когда они выступают в качестве контейнера, в котором IP-пакет переносится через составную сеть.

Для идентификации сетевых интерфейсов используют три типа адресов:

— локальные (аппаратные);

— сетевые адреса (IP-адреса);

— символьные (доменные) имена.

В большинстве технологий LAN (Ethernet, FDDI, Token Ring) для однозначной адресации интерфейсов используются ***MAC-адреса***. Существует немало технологий (X.25, ATM, frame relay), где применяются другие схемы адресации. Роль, которую играют эти адреса в TCP/IP, не зависит от того, какая именно технология используется в подсети, поэтому они имеют общее название — ***локальные (аппаратные) адреса***.

Слово «локальный» в контексте TCP/IP означает «действующий не во всей составной сети, а лишь в пределах подсети». Именно в таком смысле понимаются «локальная технология» (технология, на основе которой построена подсеть) и «локальный адрес» (адрес, используемый некой локальной технологией для адресации узлов в пределах подсети). Напомним, что в качестве подсети (локальной сети) может выступать сеть, построенная как на основе локальной технологии, например Ethernet, FDDI, так и на основе глобальной технологии, например X.25, Frame Relay. Следовательно, говоря о подсети, мы используем слово «локальная» не как характеристику технологии, на которой построена эта подсеть, а как указание на роль, которую играет эта подсеть в архитектуре составной сети.

Сложности могут возникнуть и при интерпретации слова «аппаратный». В данном случае термин «аппаратный» подчеркивает концепту-

альное представление разработчиков стека TCP/IP о подсети как о некотором вспомогательном *аппаратном* средстве, единственной функцией которого является перемещение IP-пакета через подсеть до ближайшего шлюза (маршрутизатора). И неважно, что реально нижележащая локальная технология может быть сложной, все ее сложности технологией TCP/IP игнорируются.

Чтобы технология TCP/IP могла решать свою задачу объединения сетей, ей необходима собственная глобальная система адресации, *не зависящая от способов адресации узлов в отдельных сетях.* Эта система адресации должна позволять универсальным и однозначным способом идентифицировать любой интерфейс составной сети. Очевидным решением является уникальная нумерация всех сетей составной сети, а затем нумерация всех узлов в пределах каждой из этих сетей. Пара, состоящая из ***номера сети*** и ***номера узла***, отвечает поставленным условиям, а потому может являться ***сетевым адресом***.

В качестве номера узла выступает локальный адрес этого узла (такая схема принята в стеке IPX/SPX) либо некоторое число, никак не связанное с локальной технологией, однозначно идентифицирующее узел в пределах данной подсети. В первом случае сетевой адрес становится зависимым от локальных технологий, что ограничивает его применение. Например, сетевые адреса IPX/SPX рассчитаны на работу в составных сетях, объединяющих сети, в которых используются только MAC-адреса или адреса аналогичного формата. Второй подход универсален, он характерен для стека TCP/IP. В технологии TCP/IP сетевой адрес называют ***IP-адресом***.

Если рассматривать IP-сеть, то можно отметить, что маршрутизатор по определению входит сразу в несколько сетей, следовательно, каждый его интерфейс имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов — по числу сетевых связей. Таким образом, IP-адрес идентифицирует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Каждый раз, когда пакет направляется адресату через составную сеть, в его заголовке указывается IP-адрес узла назначения. По номеру сети назначения каждый очередной маршрутизатор находит IP-адрес следующего маршрутизатора. Перед тем как отправить пакет в следующую сеть, маршрутизатор должен определить (на основании найденного IP-адреса следующего маршрутизатора) его локальный адрес.

Для этой цели протокол IP обращается к протоколу разрешения адресов (ARP):

12-B7-01-56-BA-F5 — ARP;

129.35.251.23 — IP;

www.service.telecom.com — DNS.

Заметим, что использование локального адреса в качестве номера узла имеет ряд преимуществ. Именно такая схема принята в протоколе IPv6.

Система доменных имен (DNS)

Для идентификации компьютеров аппаратное и программное обеспечение в сетях TCP/IP полагается на IP-адреса. Например, команда ftp://192.45.66.17 будет устанавливать сеанс связи с нужным ftp-сервером, а команда http://203.23.106.33 откроет начальную страницу на корпоративном веб-сервере. Пользователи предпочитают работать с более удобными ***символьными именами*** компьютеров.

Символьные идентификаторы сетевых интерфейсов (в пределах составной сети) строятся по иерархическому принципу. Составляющие полного символьного (или доменного) имени в IP-сетях разделяются точкой и перечисляются в следующем порядке: сначала простое имя хоста, затем имя группы хостов (например, имя организации), потом имя более крупной группы (домена) и так до имени домена самого высокого уровня (например, домена, объединяющего организации по географическому принципу: RU — Россия, UK Великобритания, US — США). Пример доменного имени: base2.sales.zil.ru.

Между ***доменным именем*** и IP-адресом узла нет никакой функциональной зависимости, поэтому единственный способ установить соответствие — это таблица. В сетях TCP/IP используется специальная ***система доменных имен*** (Domain Name System, DNS), которая устанавливает это соответствие на основании создаваемых администраторами сети таблиц соответствия. Поэтому доменные имена называют также ***DNS-именами***. В общем случае сетевой интерфейс может иметь несколько локальных адресов, сетевых адресов и доменных имен.

DNS (*Domain Name System* — система доменных имен) — компьютерная распределенная система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, об обслуживающих узлах для протоколов в домене (SRV-запись).

Распределенная база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определенному протоколу.

Основой DNS является представление об иерархической структуре доменного имени и *зонах*. Каждый сервер, отвечающий за имя, может *делегировать* ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за свою часть доменного имени.

DNS важна для работы Интернета, так как для соединения с узлом необходима информация о его IP-адресе, а для людей проще запоминать буквенные (обычно осмысленные) адреса, чем последовательность цифр IP-адреса. В некоторых случаях это позволяет использовать виртуальные серверы, например, HTTP-серверы, различая их по имени запроса. Первоначально преобразование между доменными и IP-адресами производилось с использованием специального текстового файла hosts, который составлялся централизованно и автоматически рассылался на каждую из машин в своей локальной сети. С ростом сети возникла необходимость в эффективном, автоматизированном механизме, которым и стала DNS.

Система DNS содержит иерархию ***DNS-серверов***, соответствующую иерархии ***зон***. Каждая ***зона*** поддерживается как минимум одним *авторитетным сервером DNS* (*authoritative* — авторитетный), на котором расположена информация о домене.

Имя и IP-адрес не тождественны — один IP-адрес может иметь множество имен, что позволяет поддерживать на одном компьютере множество веб-сайтов (это называется виртуальный хостинг). Одному имени может быть сопоставлено множество IP-адресов — это позволяет создавать балансировку нагрузки.

§ 2. Анонимность в сети Интернет

Анонимайзеры

Анонимность в сети — основная задача анонимайзеров. Всегда существует круг лиц, работающих в Интернете, которые хотели бы пользоваться возможностями глобальных сетей (желательно без ограничений) и при этом скрывать свой IP-адрес. Причины такого поведения разнообразны, причем не обязательно они связаны с преступными деяниями. Многие понимают, что чем меньше информации о вашем доступе в сеть известно другим пользователям, тем меньше шансов у злоумышленников удаленно воздействовать на ваш компьютер или использовать его для каких-то противоправных действий. К положительным момен-

там анонимного доступа в сеть можно отнести и сужение каналов доступа на компьютер спама или назойливой рекламы.

Действия преступного характера, осуществляемые анонимным пользователем в глобальной сети, имеют более широкий спектр: преступления экономические, экстремисткой направленности, методы информационных войн, приобретение запрещенной информации — это далеко не исчерпывающий перечень деяний, направленных против личности, общества, государства.

Безнаказанность некоторых противоправных действий в глобальной сети дает повод ввести на законодательном уровне запрет анонимайзеров в сети, в некоторых странах он уже существует, например, в Белоруссии. В Китайской Народной Республике установлена система «Золотой щит», выполняющая функции firewall. Учитывая напряженную международную обстановку, анонимайзеры действительно создают серьезную проблему национальной безопасности. Предложение о запрете или об ограничении работы анонимайзеров заведомо приводит к вопросу об ограничении свобод в сети Интернет, а также к вопросу о возможности технической реализации данного проекта. Тема ограничения свобод в Интернете не является предметом рассмотрения в рамках данной работы, но даже при поверхностном взгляде на эту проблему можно сделать вывод, что проблема искусственно обостряется в пределах определенного социума. Гражданин, пользуясь глобальными сетями, может прибегнуть к анонимайзерам лишь в одном случае — обезопасить обращение информации. С этой точки зрения, функцию защиты информации пользователя можно передать соответствующим государственным органам. Сформированная государственная сеть анонимайзеров сможет предоставить гарантии как надежности, так и приватности выхода в глобальную сеть. Разумеется, ни о какой анонимности со стороны государства речи быть не может, но в действительности для пользователя, который не намерен совершать неправомерные действия в Интернете, это сложно назвать недостатком. Техническая реализация проекта системы государственной сети анонимайзеров вполне осуществима, причем неофициально (в целях национальной безопасности) сеть анонимайзеров, контролируемая непосредственно государственными структурами, уже существует, о чем не раз были сообщения на различных сайтах. Однако передавать в руки государства свою конфиденциальную информацию, в том числе и коммерческую тайну, согласны далеко не все коммерчески организации, поэтому вопрос приватности в Интернете остается открытым.

Большинство анонимайзеров используют случайную цепочку узлов при передаче информации от пользователя к ресурсу и обратно. Каждому узлу в цепочке известно лишь то, от кого пришли данные, а также куда их передавать дальше, поэтому восстановить всю цепочку и отследить пользователя очень сложно. Например, по такому принципу работают анонимайзеры Tor и I2P.

Построение сетей на серверах Tor. Deep Web (Deep Net)

В данных сетях анонимность соединения гарантируется за счет серверов Tor, которые шифруют данные пользователя, перед тем как попасть во внешний мир через выходной сервер. Перенаправление распределяется случайным образом между серверами, находящимися по всему земному шару. Данные между этими серверами шифруются, если есть необходимость изменить цепочку, нужно лишь обновить соединение. Благодаря данным цепочкам вы сможете поменять свое местоположение. Данный подход обусловливает сложность в выявлении первоначального отправителя пакета информации.

Использование *Tor* сводит к минимуму нахождение вашего реального расположения на основе IP-адреса, взамен вы получаете фиктивный IP. Вы с легкостью сможете попасть на сайты, заблокированные вашим провайдером или proxy-сервером на работе (с шифрованием информации).

Пользователи сети *Tor* запускают «луковый» прокси-сервер на своей машине, который подключается к серверам *Tor*, периодически образуя цепочку сквозь сеть *Tor*, которая использует многоуровневое шифрование. Каждый пакет данных, попадающий в систему, проходит через три различных прокси-сервера — узла, которые выбираются случайным образом. Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьего узла, потом для второго и для первого. Когда первый узел получает пакет, он расшифровывает верхний слой шифра (аналогия с тем, как чистят луковицу) и узнает, куда отправить его дальше. Второй и третий серверы поступают аналогичным образом. Программное обеспечение «лукового» прокси-сервера предоставляет SOCKS-интерфейс. Программы, работающие по SOCKS-интерфейсу, могут быть настроены на работу через *Tor*, который, мультиплексируя трафик, направляет его через виртуальную цепочку *Tor* и обеспечивает анонимный веб-серфинг в сети.

Внутри сети *Tor* трафик перенаправляется от одного маршрутизатора к другому и окончательно достигает *точки выхода*, из которой чистый (нешифрованный) пакет данных доходит до изначального адреса полу-

чателя (сервера). Трафик от получателя обратно направляется в *точку выхода* сети *Tor*.

С 2004 года *Tor* может обеспечивать и анонимность для серверов, позволяя скрыть их местонахождение в Интернете при помощи специальных настроек для работы с анонимной сетью. Доступ к *скрытым службам* возможен лишь при использовании клиента *Tor* на стороне пользователя.

Скрытые службы доступны через специальные псевдо-домены верхнего уровня *.onion*. Сеть *Tor* распознает эти домены и направляет информацию анонимно к *скрытым службам*, которые обрабатывают ее посредством стандартного программного обеспечения, настроенного на прослушивание только непубличных (закрытых для внешнего доступа) интерфейсов. Отметим, что публичный Интернет чувствителен для атак соотношений, поэтому службы не являются истинно скрытыми.

Доменные имена в зоне *.onion* генерируются на основе открытого ключа сервера и состоят из 16 цифр или букв латинского алфавита. Возможно создание произвольного имени при помощи стороннего программного обеспечения.

У *скрытых сервисов Tor* есть собственные каталоги сайтов, поисковые системы, электронные торговые площадки, шлюзы интернет-трейдинга, почтовые серверы, электронные библиотеки, торрент-трекеры, блог-платформы, социальные сети, файловые хостинги, службы коротких сообщений, чат-комнаты, IRC-сети, серверы SILC, XMPP и SFTP, а также многие другие ресурсы. Ряд известных сайтов имеет свои зеркала среди *скрытых сервисов*, например, Facebook, Encyclopedia Dramatica, Библиотека Александрина, DuckDuckGo, WikiLeaks, Кавказ-Центр и Cryptocat. Существуют гейты для доступа к *скрытым сервисам* непосредственно из Интернета, а также для посещения других анонимных сетей через *Tor*.

Отметим возможность *скрытых служб Tor* размещаться за фаерволом, NAT-T, прокси-серверами и SSH, не требуя обязательного наличия публичного IP-адреса.

По оценкам экспертов, количество *скрытых сервисов Tor*, по состоянию на июль 2014 г., оценивается в 80 000–600 000 сайтов.

С мая 2005 г. анонимная сеть JAP умеет использовать узлы сети *Tor* в качестве каскада для анонимизации трафика, но только по протоколу HTTP. Это происходит автоматически в том случае, если в настройках браузера выбран SOCKS, а не HTTP-прокси. Есть возможность организовать доступ к анонимным сетям I2P, JonDonym, RetroShare, Freenet и Mixmaster непосредственно через *Tor* при помощи Whonix.

Privoxy можно настроить для обеспечения доступа к *скрытым сервисам Tor*, I2P и Freenet одновременно. Возможно совместить *Tor* и Privoxy с Hamachi, получив двойное шифрование и дополнительное скрытое туннелирование.

Ретрансляторы Tor могут быть установлены в облачном вебсервисе Amazon EC2, а также в VPS, избавляя волонтеров сети от необходимости держать ее узлы у себя дома, рискуя скомпрометировать себя.

Виртуальная частная сеть может быть запущена, используя *Tor* в качестве прозрачного прокси. Существует способ настроить файлообменную сеть WASTE для работы со *скрытыми сервисами Tor*. Система мгновенного обмена сообщениями Bitmessage может использовать *Tor* как прокси-сервер. Поисковая система YaCy может быть настроена для индексирования *скрытых сервисов Tor*. Есть возможность обеспечить анонимное использование Bitcoin при помощи *Tor*.

Один из ведущих разработчиков Bitcoin Майк Хёрн создал альтернативный протокол этой криптовалюты, названный *bitcoinj*. В отличие от оригинала, он написан на языке Java и интегрирован с сетью *Tor*, что позволяет обеспечить анонимность лиц, пользующихся кошельками или сервисами, которые принимают Bitcoin.

Исследователи из Йельского университета в работе "A TorPath to TorCoin" предложили новую альтернативную цифровую валюту *TorCoin*, основанную на модифицированном протоколе Bitcoin. Ее фундаментальное отличие от оригинала заключается в иной схеме доказательства работы, производной от пропускной способности, а не от вычислительной мощности. Чем бóльшую скорость сети сумеет обеспечить ее участник, тем значительнее вознаграждение, которое он получит. Подобная концепция особенно актуальна для *Tor*, так как анонимность и стабильность ее работы зависит от количества участников, а также интернет-трафика, которые они готовы предоставить.

Tor предназначен для скрытия факта связи между клиентом и сервером, однако он принципиально не может обеспечить полное сокрытие передаваемых данных, поскольку шифрование в данном случае является лишь средством достижения анонимности в интернете. Для сохранения более высокого уровня конфиденциальности необходима дополнительная защита самих коммуникаций. Важно и шифрование файлов, передаваемых через *Tor* (их упаковка в криптографические контейнеры и применение методов стеганографии).

Tor работает только по протоколу SOCKS, поддерживаемому не всеми приложениями, через которые может понадобиться вести аноним-

ную деятельность. Методом решения этой проблемы является использование специализированных программных прокси-серверов и аппаратных проксификаторов. Существуют отдельные способы *торификации* как различных приложений, так и операционных систем.

Tor не поддерживает UDP, что не позволяет использовать протоколы VoIP и BitTorrent без риска утечек. Эта проблема может быть решена при помощи туннелирования во Whonix и в *OnionCat*.

Сеть *Tor* не может скрыть от интернет-провайдера факт использования самой себя, так как ее адреса находятся в открытом доступе, а порождаемый ею трафик распознается с помощью снифферов и DPI. В некоторых случаях уже это становится дополнительной угрозой для пользователя. Для ее предотвращения разработчиками *Tor* были созданы средства маскировки трафика. Существуют способы скрыть использование *Tor* и при помощи VPN, SSH и *Proxy chain*.

Tor не в состоянии защитить компьютер пользователя от вредоносного шпионского программного обеспечения, которое может быть использовано для деанонимизации. Методом защиты от таких программ является применение как грамотно настроенных IPS и DLP, так и общих мер сетевой безопасности, включая расширение браузеров при вебсерфинге (например, NoScript и RequestPolicy для Firefox). Наиболее эффективным способом будет использование специализированных операционных систем, где все необходимые меры безопасности реализованы по умолчанию с учетом специфики использования *Tor*.

Использование *Tor* как шлюза на пути к всемирной сети позволяет защитить права пользователей из стран с интернет-цензурой лишь на некоторое время, ведь такой стране достаточно заблокировать доступ даже не ко всем серверам сети *Tor*, а только к центральным серверам каталогов. В этом случае энтузиастам рекомендуется настроить у себя *мостовой узел Tor*, который позволит заблокированным пользователям получить к нему доступ. На официальном сайте проекта любой пользователь всегда может найти актуальный список мостов для своей сети. Если он заблокирован, можно подписаться на официальную рассылку *Tor*, отправив письмо с темой “get bridges” на e-mail bridges@torproject.org или использовать специальный плагин для WordPress, который позволяет постоянно генерировать картинку-CAPTCHA с адресами мостов. Но даже использование таковых не является панацеей, так как с момента создания *Tor-бриджей* появилось множество способов их раскрытия.

Долговременной ключевой парой *скрытых сервисов* является RSA-1024, подверженный криптоанализу, а значит, неизбежен их переход на

другую длину ключа и/или другой асимметричный криптоалгоритм, что приведет к переименованию всех доменных имен. Поэтому в декабре 2013 г. один из ведущих специалистов The Tor Project, Inc Ник Мэтьюсон опубликовал проект спецификации для новой версии скрытых сервисов, в которой, помимо дополнительных методов их защиты от DoS-атак, планируется отказ от криптографических примитивов RSA-1024, DH-1024 и SHA-1 в пользу алгоритмов на эллиптических кривых Ed25519, Curve25519 и хеш-функции SHA-256.

Как анонимная сеть с низким временем ожидания, *Tor* потенциально уязвим к анализу трафика со стороны атакующих, которым доступны для прослушивания оба конца соединения пользователя. Согласно технической спецификации *Tor* изначально создан с расчетом на противодействие таким атакам при помощи пересылки данных фиксированными блоками в 512 байт с дальнейшим мультиплексированием в одно TLS-соединение. Группе исследователей из Люксембургского университета и RWTH удалось добиться определенных успехов в ее осуществлении. Поэтому перед использованием *Tor* необходимо выбрать *входной* и *выходной* узлы, которые находятся за пределами страны пребывания, чтобы не стать жертвой национальных программ слежения. Когда высокая анонимность в Интернете важнее скорости передачи данных, следует использовать анонимную сеть с высоким временем ожидания, например, Mixminion.

Против *Tor* могут быть использованы атаки пересечения и подтверждения, атака по времени, атака по сторонним каналам, а также *глобальное пассивное наблюдение*.

Сетевой безопасности пользователей *Tor* угрожает практическая возможность корреляции анонимного и неанонимного трафика, так как все TCP-соединения мультиплексируются в один канал. В качестве контрмеры здесь целесообразно поддерживать несколько параллельно работающих экземпляров процесса *Tor* или запустить ретранслятор этой сети.

Профессор Ангелос Керомитис из Колумбийского университета в докладе “Simulating a Global Passive Adversary for Attacking Tor-like Anonymity Systems”, представленном на конференции “Security and Privacy Day and Stony Brook” 30 мая 2008 г., описал новый способ атаки на сеть *Tor*. По его мнению, не полностью *глобальный пассивный наблюдатель* (GPA — *Global Passive Adversary*) может осуществлять наблюдение из любого участка сети с использованием новой технологии изучения трафика *LinkWidth*, который позволяет измерять пропускную

способность участков сети без кооперации с точками обмена трафиком, недосягаемыми напрямую маршрутизаторами и без сотрудничества с интернет-провайдерами. При помощи модулирования пропускной способности анонимного соединения с сервером или маршрутизатором, находящимся вне прямого контроля, исследователям удалось наблюдать получающиеся флуктуации трафика, распространяющиеся по всей сети *Tor* до конечного пользователя. Эта техника использует один из главных критериев сети *Tor* — обмен GPA-устойчивости на высокую пропускную способность и малые задержки сети. Новая техника не требует никакой компрометации узлов *Tor* или принуждения к сотрудничеству конечного сервера. Даже наблюдатель с малыми ресурсами, имеющий доступ всего к двум точкам перехвата трафика в сети, может вычислить реальный IP-адрес пользователя. Более того, высокооснащенный пассивный наблюдатель, используя топологическую карту сети *Tor*, может вычислить обратный путь до любого пользователя за 20 мин. Также исследователи утверждают, что можно вычислить IP-адрес *скрытого сервиса Tor* за 120 мин. Подобная атака возможна лишь в лабораторных условиях, так как может быть эффективно проведена только против участников сети, скачивающих большие файлы на высокой скорости через близкие друг к другу узлы при условии компрометации выходящего, что далеко от реальной работы *Tor*. Для защиты от потенциальных атак подобного рода рекомендуется не перегружать сеть, например, участием в онлайн-играх или файлообменом с пиринговыми сетями.

Ученые из Исследовательской лаборатории Военно-морских сил США и Университета Гумбольдта в 2014 г. на 21-м симпозиуме “Network and Distributed System Security Symposium” представили работу “The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network”, в которой описан механизм атаки, заключающийся в том, что клиент сети *Tor* мог посылать на ее узлы особый запрос, приводящий к нехватке памяти и аварийному завершению работы. Подобный механизм мог быть использован для организации DDoS-атак на пользователей сети *Tor*. Кроме того, его применение против *сторожевых узлов* могло привести к деанонимизации *скрытых сервисов*. При этом сам атакующий мог оставаться анонимным, прикрываясь сетью. Уязвимость, позволявшая осуществлять подобную атаку, была закрыта в версии *Tor*, начиная с 0.2.4.18-rc.

В апреле 2014 г. сеть *Tor* оказалась в числе сервисов, подверженных уязвимости Heartbleed. Исследователь Колин Мулинер из Северо-Восточного университета протестировал *ретрансляторы Tor* с помо-

щью опубликованного эксплоита и пришел к выводу, что не менее 20% из них уязвимы. В The Tor Project, Inc приняли решение о принудительном отключении этих узлов, что привело к существенному сокращению пропускной способности сети. По мнению Руны Сандвик, Heartbleed стала самой серьезной на тот момент технической проблемой в истории проекта *Tor*.

В мае 2014 г. группой ученых из Люксембургского университета в работе "Deanonymisation of clients in Bitcoin P2P network" была представлена технология деанонимизации пользователей Bitcoin, находящихся за NAT и работающих через *Tor*. Эта методика использует уязвимость протокола криптовалюты, которая позволяет клиентам осуществлять свободный сбор статистики и выбор произвольных узлов. Поэтому атакующий, используя даже незначительное количество случайных соединений, может собрать достаточно информации для последующего датамайнинга и различения участников сети. После накопления определенного массива данных, применяя DoS-атаку на сеть Bitcoin, можно деанонимизировать не менее половины ее пользователей. Так как в системе Bitcoin по умолчанию применяется банк IP-адресов, причастных к DoS-атакам, ее применение через *выходные узлы Tor* позволяет последовательно выводить из строя клиентов, работающих через эту анонимную сеть. Следовательно, становится возможным выделение тех из них, которые не работают с клиентом, выходящим в сеть через *Tor*. Опасность этой атаки заключается в том, что она работает, даже если соединения с Bitcoin зашифрованы, ее побочным эффектом является упрощение нечестного майнинга путем манипуляции цепочками блоков.

В *Tor* неоднократно обнаруживались программные ошибки, способные разрушить анонимность пользователя, но благодаря открытости проекта они оперативно устраняются.

ЗАКЛЮЧЕНИЕ

Современные технологии обработки информации на компьютере существенным образом изменили представление об информационных технологиях. Их результатом стали обработка и хранение самой информации пользователя в компьютерном формате, воспроизведение которого невозможно с использованием только органов восприятия человека. Обязательное дополнение пользовательской информации — метаданные об информации, т. е. служебные данные о дате, времени, месте создания и редактирования файла и пр. Исследование этих сведений с высокой вероятностью может позволить получить дополнительные характеристики.

Современные сетевые технологии основаны на протоколах, созданных более 20 лет назад, что обусловило, с одной стороны, их широкое применение, с другой — практическую невозможность замены при большом распространении рабочих станций в сети. Данные протоколы определяют возможность установления адреса отправителей почтовых сообщений, физического определения места нахождения сайтов и т. д. Анонимность пользователя в сети может быть реализована и через сайты анонимайзеров.

Таким образом, знания и умения исследовать результаты работы компьютерных технологий обработки информации приобретают все большее значение. Современное развитие общества неразрывно связано с повышением роли процессов информатизации, которые выражаются в широком распространении разнообразных носителей информации в компьютерном формате хранения и в лавинообразном накоплении информации в базах данных операторов информационных сетей.

ОГЛАВЛЕНИЕ

Учебное издание

Горев Александр Иванович
Симаков Александр Александрович

ОБРАБОТКА И ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Редактор Ю. А. Прудникова
Корректор Л. И. Замулло
Технический редактор Л. А. Янцен
ИД № 03160 от 02 ноября 2000 г.
Подписано в печать 15.12.2016. Формат 60x84/16. Бумага офсетная № 1. Усл. печ. л. 5,1.
Уч.-изд. л. 4,3. Тираж 110 экз. Заказ № 674.

Редакционно-издательский отдел
Группа полиграфической и оперативной печати
644092, г. Омск, пр-т Комарова, д. 7