

Внутреннее устройство Windows

Ключевые компоненты и возможности

Седьмое издание

Марк Руссинович

Дэвид Соломон

Алекс Ионеску

Андреа Аллиев



Санкт-Петербург • Москва • Минск

2025

Оглавление

Об авторах этого издания	16
Предисловие	18
Введение	21
История серии	21
Изменения в седьмом издании	22
Изменения в томе 2	23
Практические эксперименты	23
Незатронутые темы	23
Предупреждение и предостережение	24
Чего мы ожидаем от читателя	24
Структура книги	24
Шрифтовые выделения	25
Благодарности	25
Остаемся на связи	27
От издательства	27
Глава 8. Системные механизмы	28
Модель выполнения кода процессором	29
Сегментация	29
Сегменты состояния задач	34
Аппаратные уязвимости к атакам по сторонним каналам	37
Внеочередное выполнение команд	38
Блок предсказания переходов	39
Кэш процессора	40
Атаки по сторонним каналам	42
Меры борьбы с атаками по сторонним каналам в Windows	46
Затенение KVA	47
Аппаратный контроль не прямых переходов (IBRS, IBPB, STIBP, SSBD)	51
Retpoline и оптимизация импорта	53
Сопряжение STIBP	57

Диспетчеризация системных прерываний	61
Диспетчеризация прерываний	63
Конвейерные и иницируемые сообщениями прерывания.....	84
Обработка таймера	103
Системные рабочие потоки	120
Управление исключениями.....	125
Обработка действий системных служб.....	132
WoW64 (Windows-on-Windows)	147
Ядро WoW64.....	148
Перенаправление путей в файловой системе	152
Перенаправление в системном реестре.....	154
Симуляция X86 на платформах AMD64.....	155
ARM.....	157
Модели памяти	157
Симуляция ARM32 на платформах ARM64.....	158
Симуляция x86 на платформах ARM64	159
Диспетчер объектов	169
Объекты исполнительной системы	172
Структура объектов	176
Синхронизация	222
Высокоуровневая IRQL-синхронизация.....	223
Низкоуровневая IRQL-синхронизация.....	230
Продвинутый локальный вызов процедур.....	267
Модель подключения.....	268
Модель сообщений.....	270
Асинхронные операции	273
Просмотры, области и разделы	274
Атрибуты.....	275
Двоичные объекты, дескрипторы и ресурсы.....	276
Передача дескрипторов.....	277
Безопасность.....	279
Производительность.....	280
Управление электропитанием.....	281
Атрибут прямого события ALPC	282
Отладка и трассировка.....	282
Средство уведомлений Windows	284
Возможности WNF	285
Пользователи WNF.....	286
Именованные состояния WNF и хранение	292
Агрегация событий WNF	297
Отладка в пользовательском режиме.....	299
Поддержка со стороны ядра.....	299

Платформенно-зависимая поддержка.....	301
Поддержка подсистемы Windows.....	303
Пакетные приложения.....	304
Приложения UWP.....	306
Приложения Centennial.....	307
Диспетчер активности хоста.....	311
Репозиторий состояний.....	313
Мини-репозиторий зависимостей.....	317
Фоновые задачи и инфраструктура брокеров.....	318
Установка и запуск пакетных приложений.....	321
Активация пакетов.....	321
Регистрация пакетов.....	328
Заключение.....	330
Глава 9. Технологии виртуализации.....	331
Гипервизор Windows.....	331
Разделы, процессы и потоки.....	333
Запуск гипервизора.....	338
Диспетчер памяти гипервизора.....	344
Планировщики Hyper-V.....	353
Гипервызовы и TLFS гипервизора.....	365
Перехваты.....	367
Синтетический контроллер прерываний.....	368
API платформы гипервизора Windows и разделы EXO.....	371
Вложенная виртуализация.....	374
Гипервизор Windows на ARM64.....	382
Стек виртуализации.....	383
Служба диспетчера виртуальных машин и рабочие процессы.....	384
Драйвер VID и диспетчер памяти стека виртуализации.....	386
Работа виртуальной машины.....	387
VMBus.....	393
Первичный обмен квитирующими сообщениями VMBus.....	394
Поддержка виртуального оборудования.....	400
Виртуальные машины с поддержкой VA.....	408
Безопасность на основе виртуализации (VBS).....	413
Виртуальные уровни доверия и виртуальный безопасный режим.....	414
Сервисы, предоставляемые VSM, и требования.....	416
Безопасное ядро (Secure Kernel).....	419
Виртуальные прерывания.....	420
Безопасный перехват.....	423
Системные вызовы VSM.....	425
Защищенные потоки и планирование.....	432

Hypervisor-Enforced Code Integrity (HVCI)	435
Виртуализация UEFI во время выполнения	435
Запуск VSM	437
Диспетчер памяти безопасного ядра	441
Горячее исправление	447
Изолированный пользовательский режим	450
Создание траслетов	451
Защищенные устройства	455
Анклав на основе VBS	458
Аттестация среды выполнения System Guard	466
Заключение	471
Глава 10. Управление, диагностика и трассировка	472
Реестр	472
Просмотр и изменение реестра	472
Использование реестра	473
Типы данных реестра	474
Логическая структура реестра	475
Кусты приложений	484
Расширение для работы с реестром в режиме транзакций — Transactional Registry (TxR)	486
Мониторинг активности реестра	487
Внутреннее устройство Process Monitor	488
Внутреннее устройство реестра	489
Реорганизация кустов	499
Пространство имен и работа реестра	500
Обеспечение надежного хранения	503
Фильтрация реестра	508
Виртуализация реестра	508
Оптимизация реестра	512
Службы Windows	512
Приложения служб	513
Учетные записи служб	522
Диспетчер управления службами	536
Программы управления службами	541
Запуск служб	542
Службы с отложенным автозапуском	549
Службы с запуском по триггеру	549
Ошибки, возникающие при запуске	551
Признание загрузки и последняя удачная конфигурация	552

Сбой служб.....	554
Завершение работы служб.....	556
Процессы, общие для нескольких служб.....	557
Теги служб.....	561
Пользовательские службы.....	562
Пакетные службы	566
Защищенные службы	566
Планирование задач и UBRM.....	569
Планировщик задач	569
Унифицированный диспетчер фоновых процессов	576
СОМ-интерфейсы планировщика задач	581
Инструментарий управления Windows	582
Архитектура WMI	582
Поставщики WMI	584
Общая информационная модель и язык формата управляемых объектов	585
Связи классов.....	589
Реализация WMI	592
Безопасность WMI.....	594
Трассировка событий для Windows	594
Инициализация ETW	597
Сеансы ETW	599
Поставщики ETW.....	602
Поставка событий.....	607
Поток ETW Logger	608
Потребление событий.....	610
Системные средства ведения журнала (логгеры)	614
Безопасность ETW	621
Динамическая трассировка.....	625
Внутренняя архитектура.....	628
Библиотека типов DTrace.....	635
Отчеты об ошибках Windows.....	637
Сбой пользовательского приложения.....	638
Сбой в режиме ядра (системы)	645
Обнаружение зависания процесса	655
Глобальные флаги	658
Прослойки ядра.....	661
Инициализация механизма прослоек.....	662
База данных прослоек	664
Прослойки драйверов.....	665
Прослойки устройств	669
Заключение.....	669

Глава 11. Кэширование и файловые системы	670
Терминология	670
Ключевые функции диспетчера кэша	672
Единый централизованный системный кэш	672
Диспетчер памяти	672
Когерентность кэша	673
Виртуальное блочное кэширование	674
Потоковое кэширование	675
Поддержка восстанавливаемых файловых систем	675
Усовершенствования рабочего набора NTFS MFT	676
Поддержка разделов памяти	677
Управление виртуальной памятью кэша	678
Размер кэша	680
Виртуальный размер кэша	680
Размер рабочего набора кэша	680
Физический размер кэша	681
Структуры данных кэша	683
Общесистемные структуры данных кэша	683
Структуры данных кэша для отдельного файла	686
Интерфейсы файловой системы	689
Копирование в кэш и из него	691
Кэширование с помощью интерфейсов отображения и закрепления	691
Кэширование с помощью интерфейсов прямого доступа к памяти	692
Быстрый ввод-вывод	692
Чтение с упреждением и отложенная запись	694
Интеллектуальное упреждающее чтение	694
Усовершенствования, связанные с упреждающим чтением	696
Кэширование с отложенной записью и поздняя запись	697
Отключение поздней записи для файла	703
Принудительная запись кэша на диск	704
Сброс отображенных файлов на диск	704
Дросселирование записи	705
Системные потоки	706
Агрессивная отложенная запись и низкоприоритетная поздняя запись	707
Динамическая память	708
Учет дисковых операций ввода-вывода в диспетчере кэша	709
Файловые системы	711
Форматы файловой системы Windows	712
CDFS	712
UDF	712
FAT12, FAT16 и FAT32	713

exFAT	716
NTFS	717
ReFS	718
Архитектура драйвера файловой системы	719
Локальные FSD	719
Сетевые FSD	721
Операции с файловой системой	728
Явный файловый ввод-вывод	729
Запись измененной и отображенной страницы диспетчера памяти	733
Система поздней записи диспетчера кэша	733
Поток упреждающего чтения диспетчера кэша	734
Обработчик отказов страниц диспетчера памяти	734
Драйверы фильтров файловой системы и мини-фильтры	735
Фильтрация именованных каналов и мейлслоты	736
Управление поведением точки повторной обработки	737
Process Monitor	739
Файловая система NT	740
Требования к файловой системе высокого класса	741
Восстанавливаемость	741
Безопасность	741
Резервирование данных и отказоустойчивость	742
Дополнительные возможности NTFS	742
Несколько потоков данных	743
Имена на основе Юникода	745
Общее средство индексирования	746
Динамическое перераспределение плохих кластеров	746
Жесткие ссылки	746
Символические (мягкие) ссылки и соединения	747
Сжатие и разреженные файлы	750
Регистрация изменений	751
Пользовательские квоты в томе	752
Отслеживание ссылок	752
Шифрование	753
Семантика удаления в стиле POSIX	754
Дефрагментация	757
Динамическая разбивка на разделы	760
Поддержка NTFS для многоуровневых томов	762
Драйвер файловой системы NTFS	766
Структура NTFS на диске	769
Томы	769
Кластеры	770

Главная файловая таблица	771
Номера файловых записей	775
Файловые записи	776
Имена файлов	779
Туннелирование	782
Резидентные и нерезидентные атрибуты	783
Сжатие данных и разреженные файлы	787
Сжатие разреженных данных	787
Сжатие неразреженных данных	789
Разреженные файлы	791
Файл журнала изменений	791
Индексирование	796
Идентификаторы объектов	798
Контроль над квотами	799
Консолидированная безопасность	800
Точки повторной обработки	801
Storage Reserves и NTFS Reservations	803
Поддержка транзакций	806
Изоляция	807
Транзакционные API	808
Реализация на диске	809
Реализация протоколирования	812
Поддержка восстановления NTFS	812
Конструкция	813
Регистрация метаданных	814
Служба файла журнала	814
Типы записей в журнале	816
Восстановление	819
Проход анализа	819
Проход повтора	820
Проход отмены	821
Восстановление плохих кластеров NTFS	823
Самовосстановление	827
Проверка диска в режиме онлайн и быстрое восстановление	828
Зашифрованная файловая система	831
Первичное шифрование файла	834
Процесс расшифровки	837
Резервное копирование зашифрованных файлов	837
Копирование зашифрованных файлов	838
Передача шифрования в BitLocker	839
Поддержка шифрования в режиме онлайн	840

Диски с прямым доступом	842
Модель драйвера DAX	844
Тома DAX	845
Кэшированный и некэшированный ввод-вывод в томах DAX	846
Отображение исполняемых образов	847
Блочные тома	851
Драйверы фильтров файловой системы и DAX	852
Сброс ввода-вывода в режиме DAX	854
Поддержка больших и огромных страниц	855
Поддержка виртуальных дисков постоянной памяти и Storage Spaces	859
Устойчивая файловая система	863
Архитектура Minstore	864
Физическая схема B ⁺ -дерева	866
Распределители	867
Таблица страниц	870
Ввод-вывод Minstore	871
Архитектура ReFS	873
Дисковая структура ReFS	877
Идентификаторы объектов	878
Безопасность и журнал изменений	879
Расширенные возможности ReFS	880
Клонирование блоков файлов (поддержка моментальных снимков) и разреженный VDL	880
Сквозная запись в ReFS	883
Поддержка восстановления ReFS	885
Обнаружение утечек	887
Тома магнитной записи внахлест	888
Поддержка ReFS для многоуровневых томов и SMR	890
Уплотнение контейнеров	893
Сжатие и фантомные файлы	896
Storage Spaces	897
Внутренняя архитектура Storage Spaces	898
Услуги, предоставляемые Storage Spaces	899
Заключение	903
Глава 12. Запуск и завершение работы системы	905
Процесс загрузки	905
Загрузка UEFI	906
Процесс загрузки BIOS	910
Безопасная загрузка	910
Диспетчер загрузки Windows	914

Меню загрузки.....	933
Запуск загрузочного приложения.....	934
Измеренная загрузка.....	935
Доверенное исполнение.....	940
Загрузчик операционной системы Windows.....	943
Загрузка из iSCSI.....	946
Загрузчик гипервизора.....	947
Политика запуска VSM.....	949
Безопасный запуск.....	952
Инициализация ядра и исполнительных подсистем.....	955
Фаза 1 инициализации ядра.....	961
Smss, Csrss и Wininit.....	967
ReadyBoot.....	972
Автоматически запускаемые образы.....	974
Завершение работы.....	975
Спящий режим и быстрый запуск.....	979
Среда восстановления Windows (WinRE).....	984
Безопасный режим.....	986
Загрузка драйвера в безопасном режиме.....	988
Пользовательские программы с поддержкой безопасного режима.....	990
Файл состояния загрузки.....	990
Заключение.....	991