Operating Systems & Security

2024

Антонов ДМ

Часть 1. Общая информация об ОС

Часть 2. Основные понятия и документы по безопасности ОС

Часть 3. Основные инструменты обеспечения безопасности ОС

Часть 4. Безопасность в ОС Windows

Часть 5. Безопасность в ОС Unix/Linux

Часть 6. Безопасность в других ОС

Часть 1

1. Понятие ОС
2. Виды ОС
3. Назначение и основы работы ОС
4. Структура ОС
5. Виртуализация

ИНТЕРЕСНЫЕ ССЫЛКИ

Raspberry Pi Pico взламывает BitLocker менее чем за минуту
https://www.securitylab.ru/news/545874.php?utm_referrer=https%3A%2F%2Fwww.securitylab.ru%2Fnews%2Fpage1_2.php

Призраки в сети: RedCurl снова на охоте
https://www.securitylab.ru/news/545859.php

Я твой рот ломал: 3 млн. зубных щеток использовались в DDoS-атаке
https://www.securitylab.ru/news/545870.php

77% российских компаний недостаточно защищены от взлома
https://cisoclub.ru/77-rossijskih-kompanij-nedostatochno-zashhishheny-ot-vzloma/

Инструмент для уведомления об ошибках Windows используется в кибератаках
https://www.anti-malware.ru/news/2023-01-06-1447/40254

Эксперты из Китая взломали RSA-шифрование с помощью квантовых компьютеров
https://www.anti-malware.ru/news/2023-01-06-1447/40255

ИСТОЧНИКИ ИНФОРМАЦИИ

1) Марк Руссинович. Внутреннее устройство Windows. 7-е изд

https://learn.microsoft.com/ru-ru/sysinternals/resources/windows-internals

2) Microsoft Windows Server 2022. Полное руководство

3) Столлингс Вильям. Операционные системы: Внутренняя структура и принципы проектирования [2020]

4) Windows 10. Новейший самоучитель. 3-е издание

5) Ратбон Энди Windows 10 для чайников [2016]

6) Колисниченко Денис. Самоучитель Microsoft Windows 11

7) Павел Йосифович Работа с ядром Windows [2021]

….

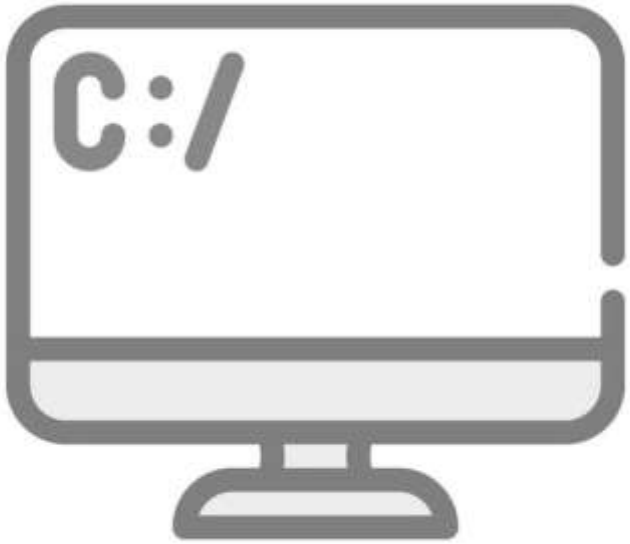
https://learn.microsoft.com/ru-ru/windows/resources/

Образы Windows
https://www.microsoft.com/ru-ru/software-download/windows11
https://techbench.betaworld.cn/products.php
https://tb.rg-adguard.net/public.php

БЕЗОПАСНОСТЬ БЕЗОПАСНОСТИ

Что понимать под термином

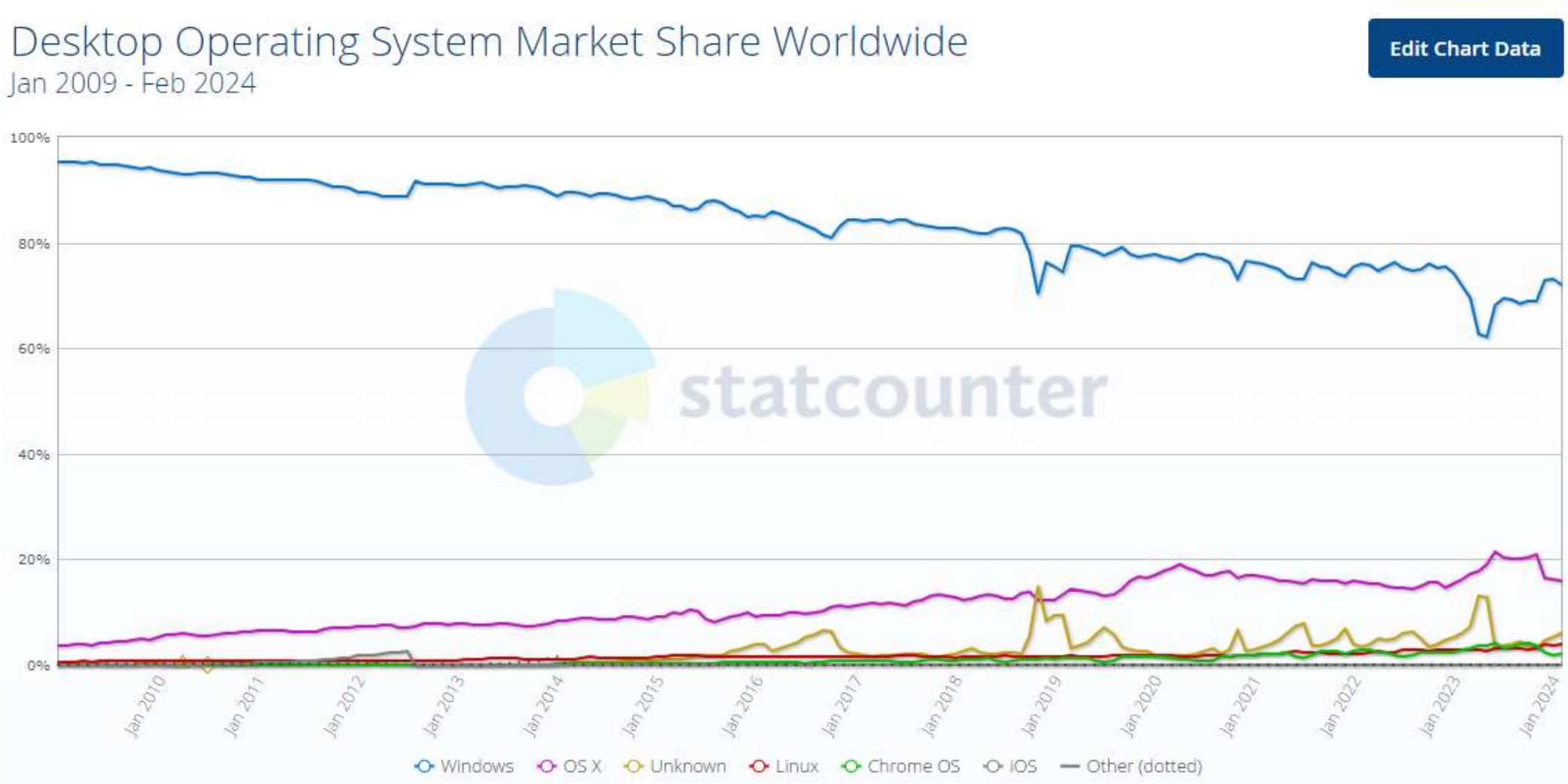
Система?
Операционная система?
Безопасная система?
Безопасная операционная система?



СТАТИСТИКА

https://gs.statcounter.com/os-market-share#monthly-200901-202402

СТАТИСТИКА



И?

https://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-200901-202402

СТАТИСТИКА

https://gs.statcounter.com/windows-version-market-share/desktop/worldwide/#monthly-201007-202402

НАЗНАЧЕНИЕ И ФУНКЦИИ

Основные функции ОС:

- управление устройствами компьютера (ресурсами);
- управление процессами;
- управление доступом к данным на энергонезависимых носителях;
- ведение файловой структуры;
- пользовательский интерфейс

Назначение ОС - организация вычислительного процесса в ВС, рациональное распределение вычислительных ресурсов между отдельными решаемыми задачами; предоставление пользователям сервисных средств, для процесса программирования и отладки задач.

КЛАССИФИКАЦИЯ

По особенностям управления ресурсами

- Поддержка многозадачности
- Характер многозадачности
- Поддержка многопотоковости
- Поддержка многопользова-тельского режима
- Поддержка много-процессорности

По особенностям аппаратных платформ

- Персональных компьютеров
- Миникомпьютеров
- Мэйнфреймов
- Кластеров
- Сетей ЭВМ

По особенностям областей использования

- Системы пакетной обработки
- Системы разделения времени
- Системы реального времени

По особенностям построения ядра

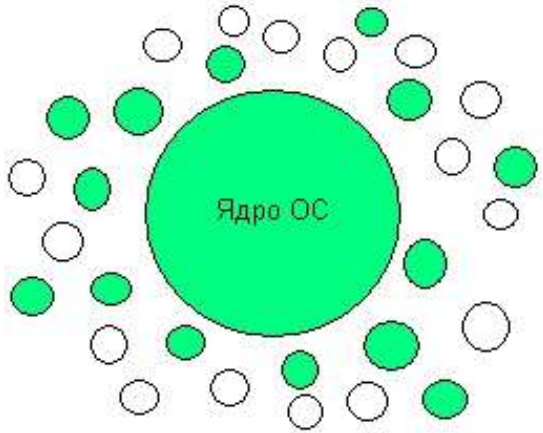
- Монолитное ядро
- Могослойное ядро
- Микроядро
- Экзоядро

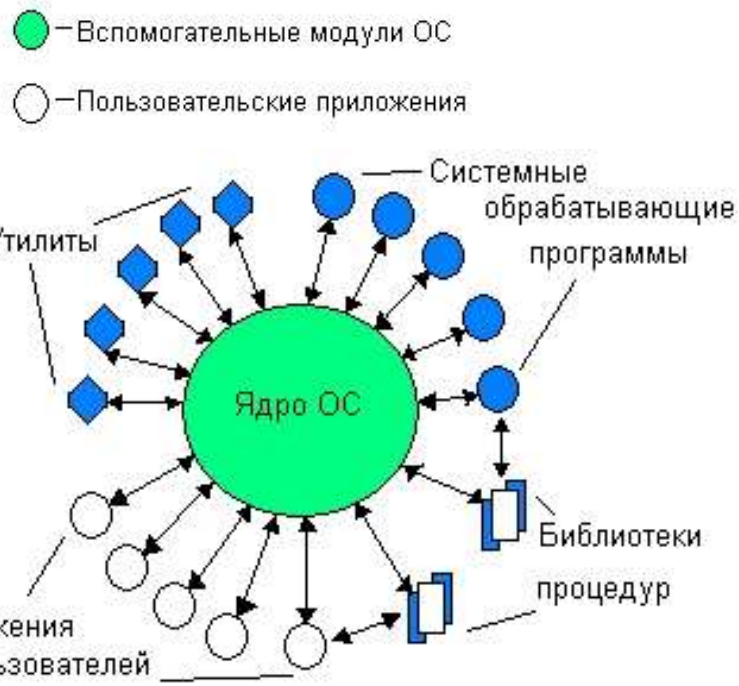
И?

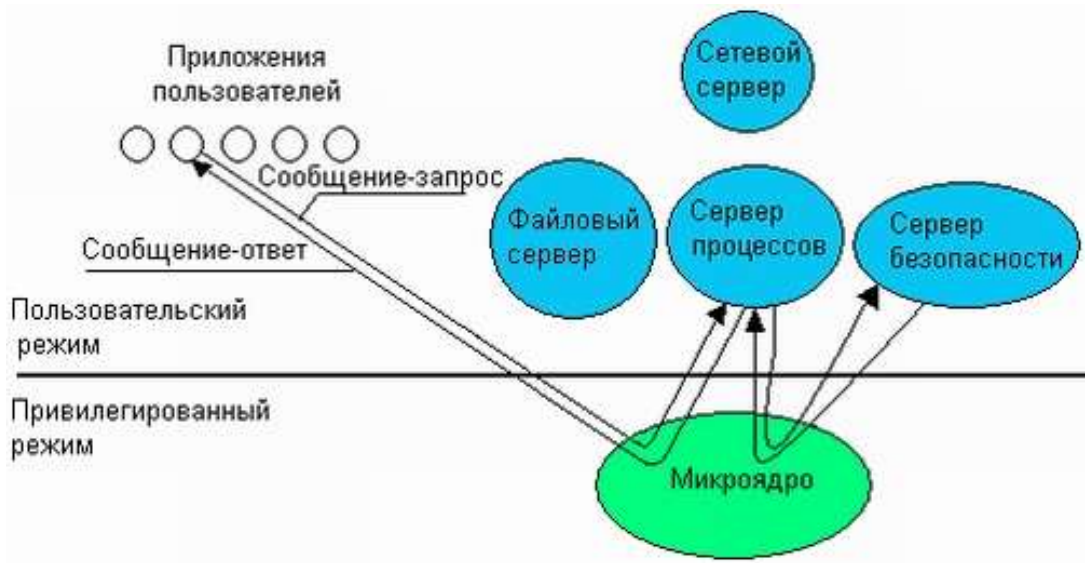
http://citforum.ru/operating_systems/sos/contents.shtml

Сетевые операционные системы *Н. А. Олифер, В. Г. Олифер*

СТРУКТУРА



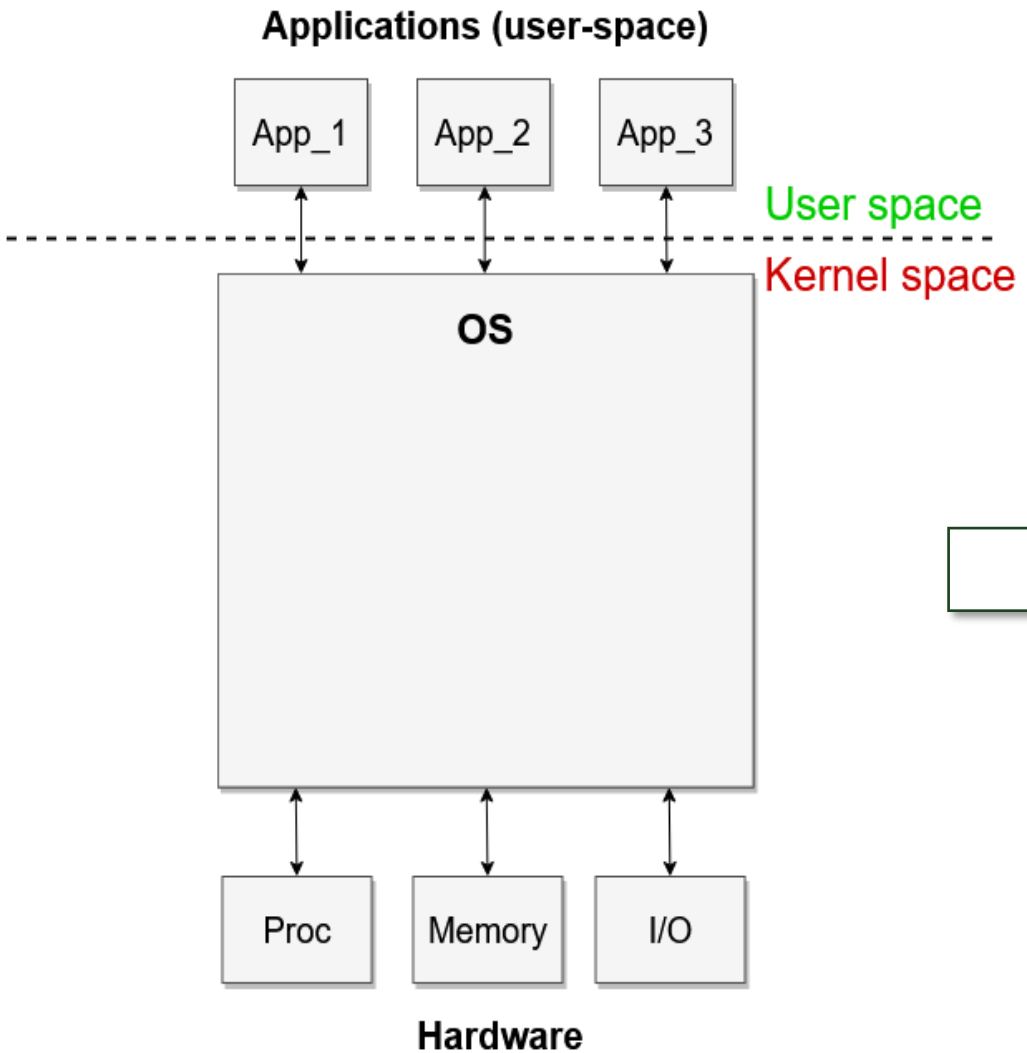


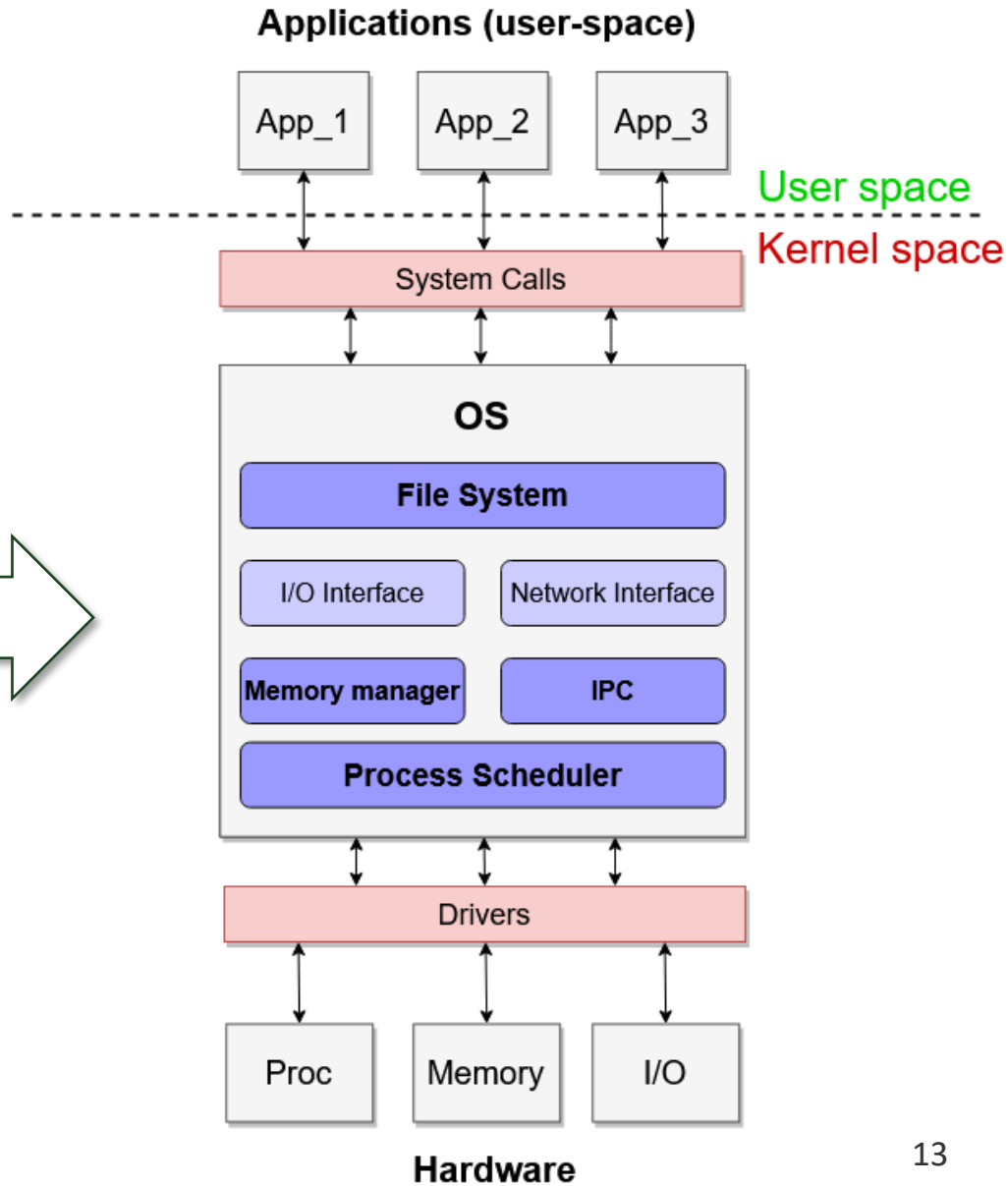


http://citforum.ru/operating_systems/sos/contents.shtml

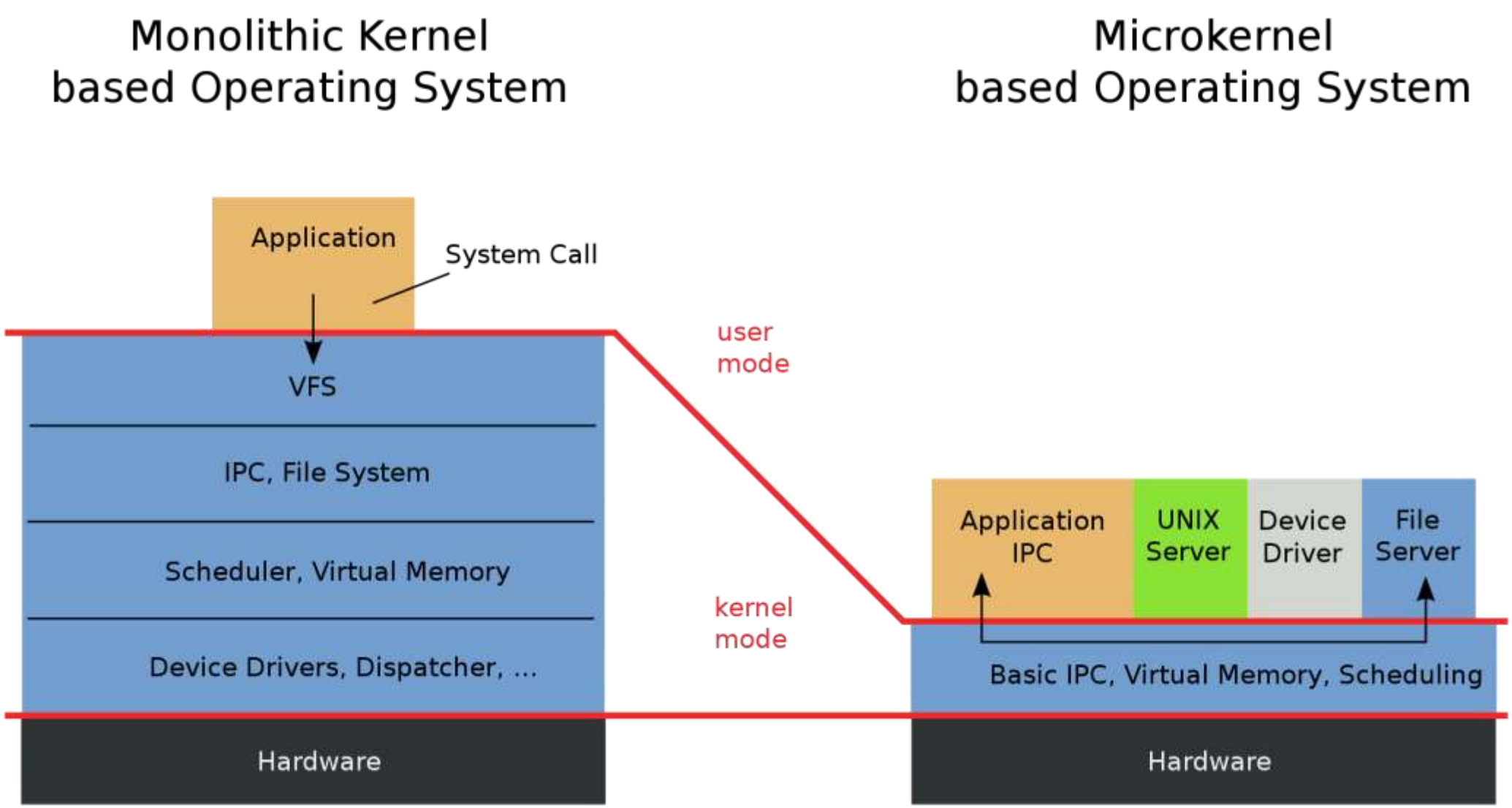
Сетевые операционные системы *Н. А. Олифер, В. Г. Олифер*

СТРУКТУРА


Applications (user-space)
App_1
App_2
App_3
User space
Kernel space
OS
Proc
Memory
I/O
Hardware


Applications (user-space)
App_1
App_2
App_3
User space
Kernel space
System Calls
OS
File System
I/O Interface
Network Interface
Memory manager
IPC
Process Scheduler
Drivers
Proc
Memory
I/O
Hardware

СТРУКТУРА ЯДРА



СТРУКТУРА ЯДРА

Ядра ОС бывают трех типов:

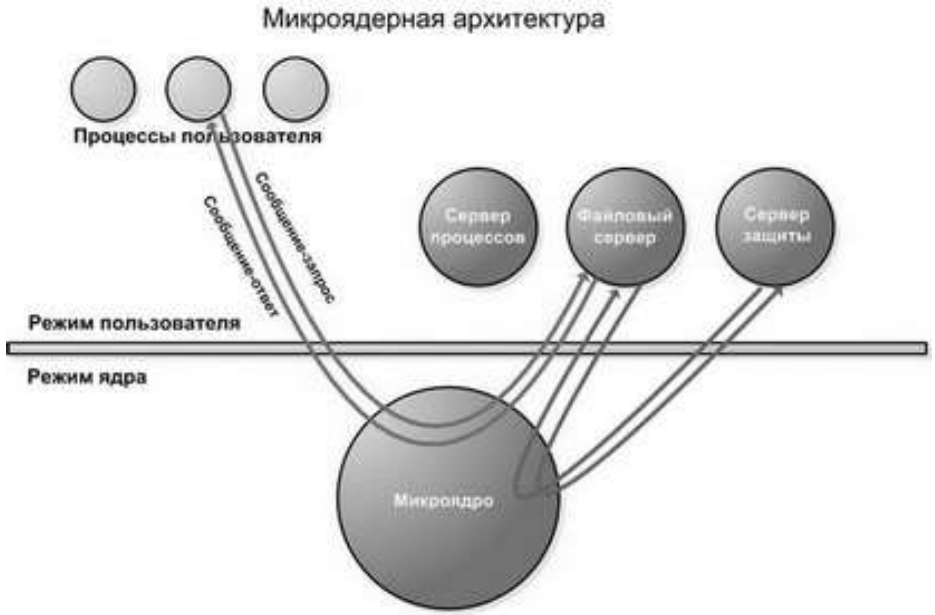
- микроядро;
- монолит (Linux);
- гибрид (OS X, Windows).

Основная разница между монолитным и микроядром в том, что микроядра включают только:
IPC (систему межпроцессного взаимодействия), управление памятью, планировщик и диспетчер.

В то время как монолитные ядра также включают в себя:
Файловую систему (системы), драйвера, VFS (в случае с Linux kernel).

Ядро Линукса занимается:

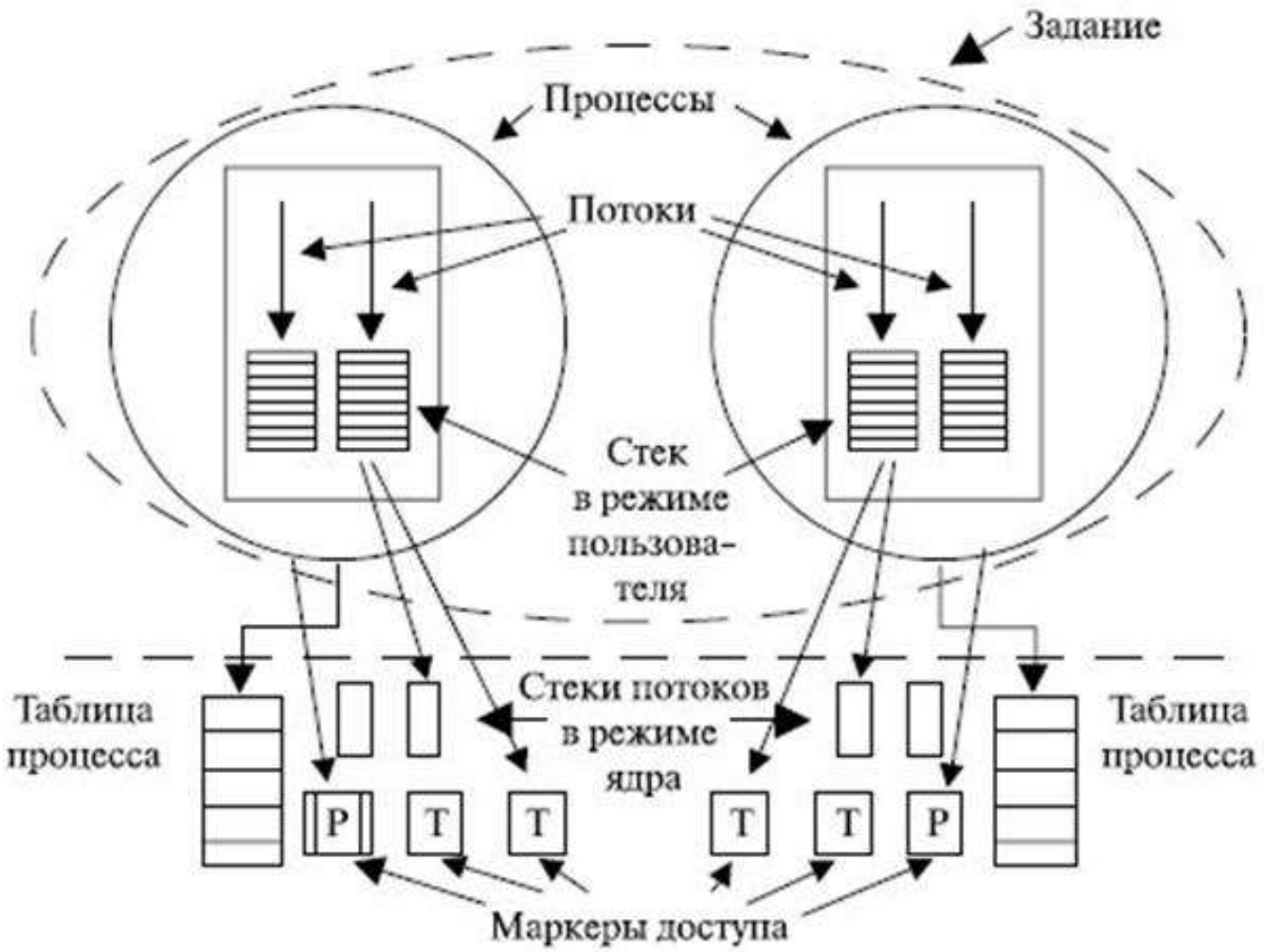
- Управлением процессами.
- Управлением памятью.
- Взаимодействием с устройствами (через драйвера).
- Системными вызовами и безопасностью.



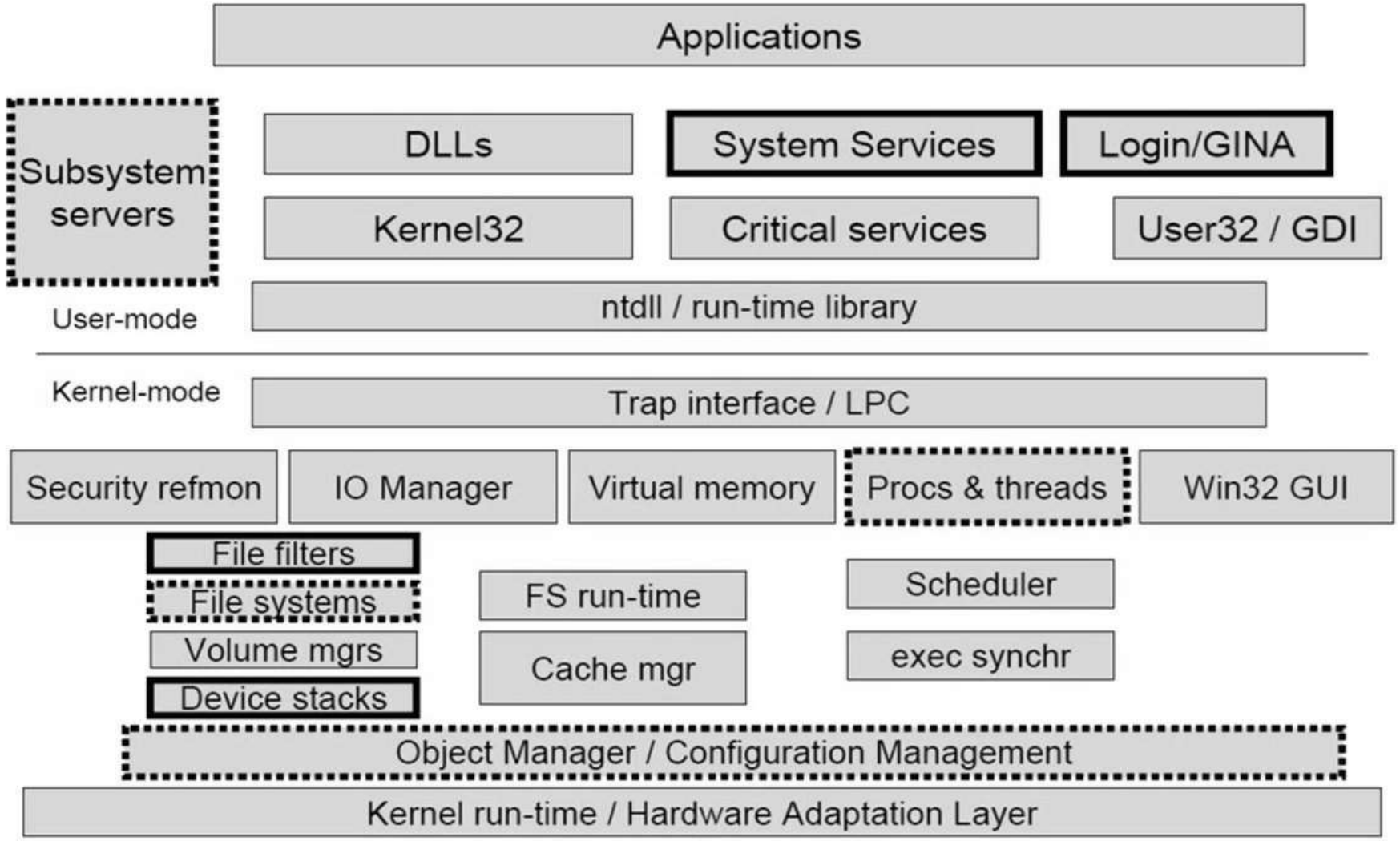
ОБЪЕКТЫ

Объекты ОС

- процессы,
- файлы,
- события,
- потоки,
- семафоры,
- мьютексы,
- каналы,
- файлы, проецируемые в память



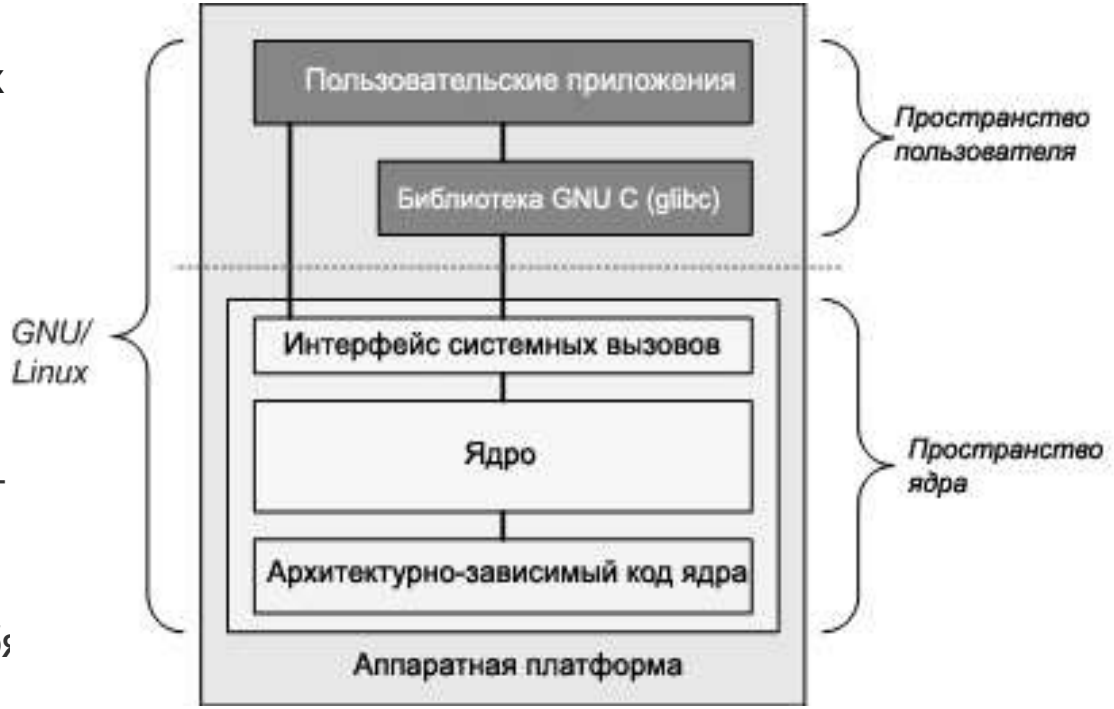
СТРУКТУРА WINDOWS



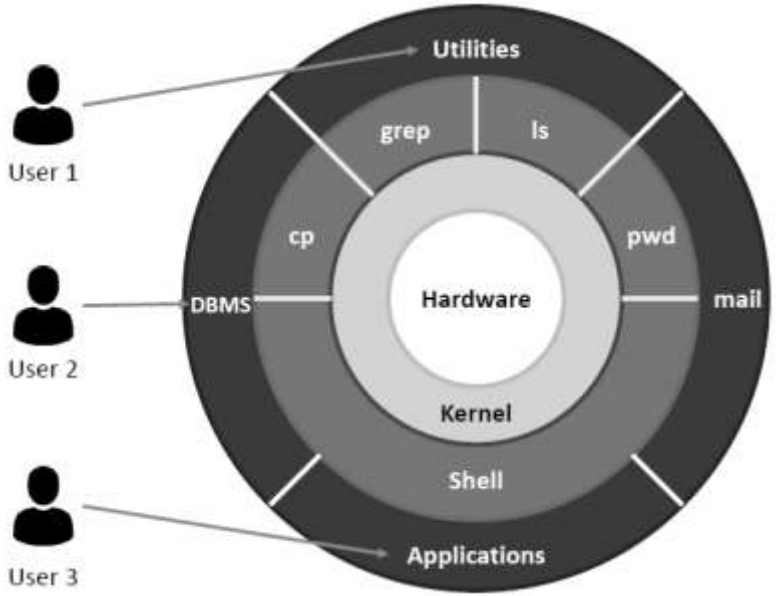
LINUX

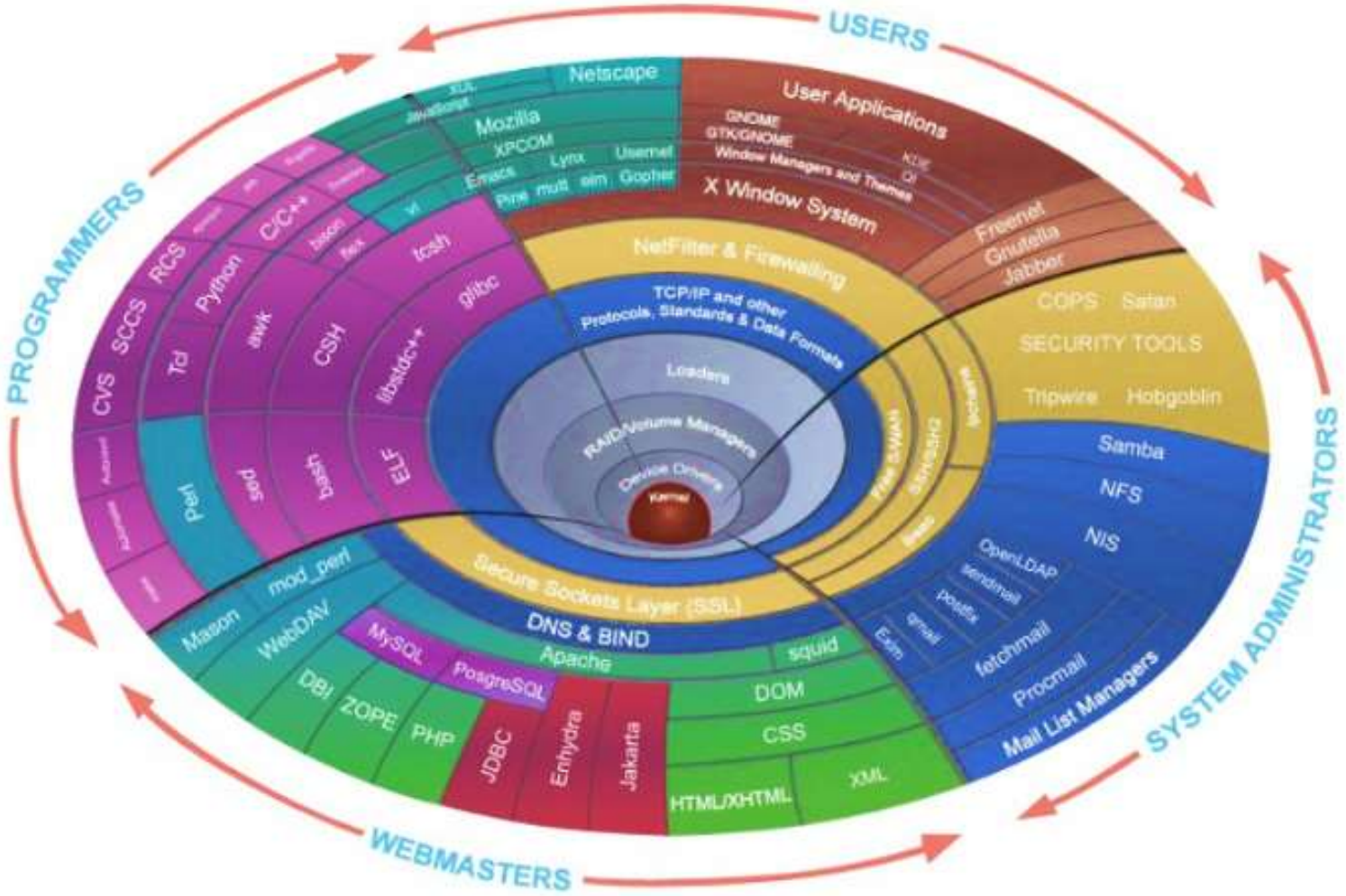
Linux-системы реализуются на модульных принципах, стандартах и соглашениях, заложенных в Unix в течение 1970-х и 1980-х годов. Такая система использует монолитное ядро, которое управляет процессами, сетевыми функциями, периферией и доступом к файловой системе. Драйверы устройств либо интегрированы непосредственно в ядро, либо добавлены в виде модулей, загружаемых во время работы системы.

Отдельные программы, взаимодействуя с ядром, обеспечивают функции системы более высокого уровня.
Например, пользовательские компоненты GNU являются важной частью большинства Линукс-систем, включающей в себя наиболее распространённые реализации библиотеки языка Си, популярных оболочек операционной системы, и многих других общих инструментов Unix, которые выполняют многие основные задачи операционной системы.
Графический интерфейс пользователя (или GUI) в большинстве систем Linux построен на основе X Window System, реже на основе более современного Wayland.



ЯДРО LINUX



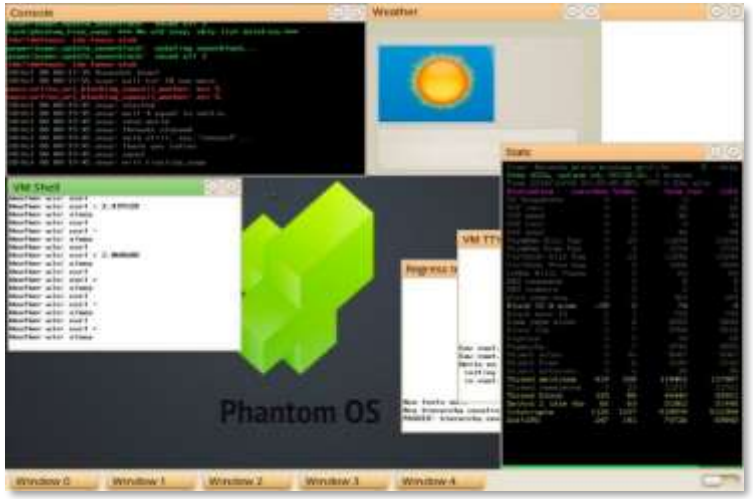


Подробности релиза ядра Linux 6.7.
https://habr.com/ru/news/784982/

Производительность TCP в Linux выросла на 40%
Подробнее: https://www.securitylab.ru/news/545200.php?ysclid=lsfzamypb6978134068&utm_referrer=https%3A%2F%2Fya.ru%2F

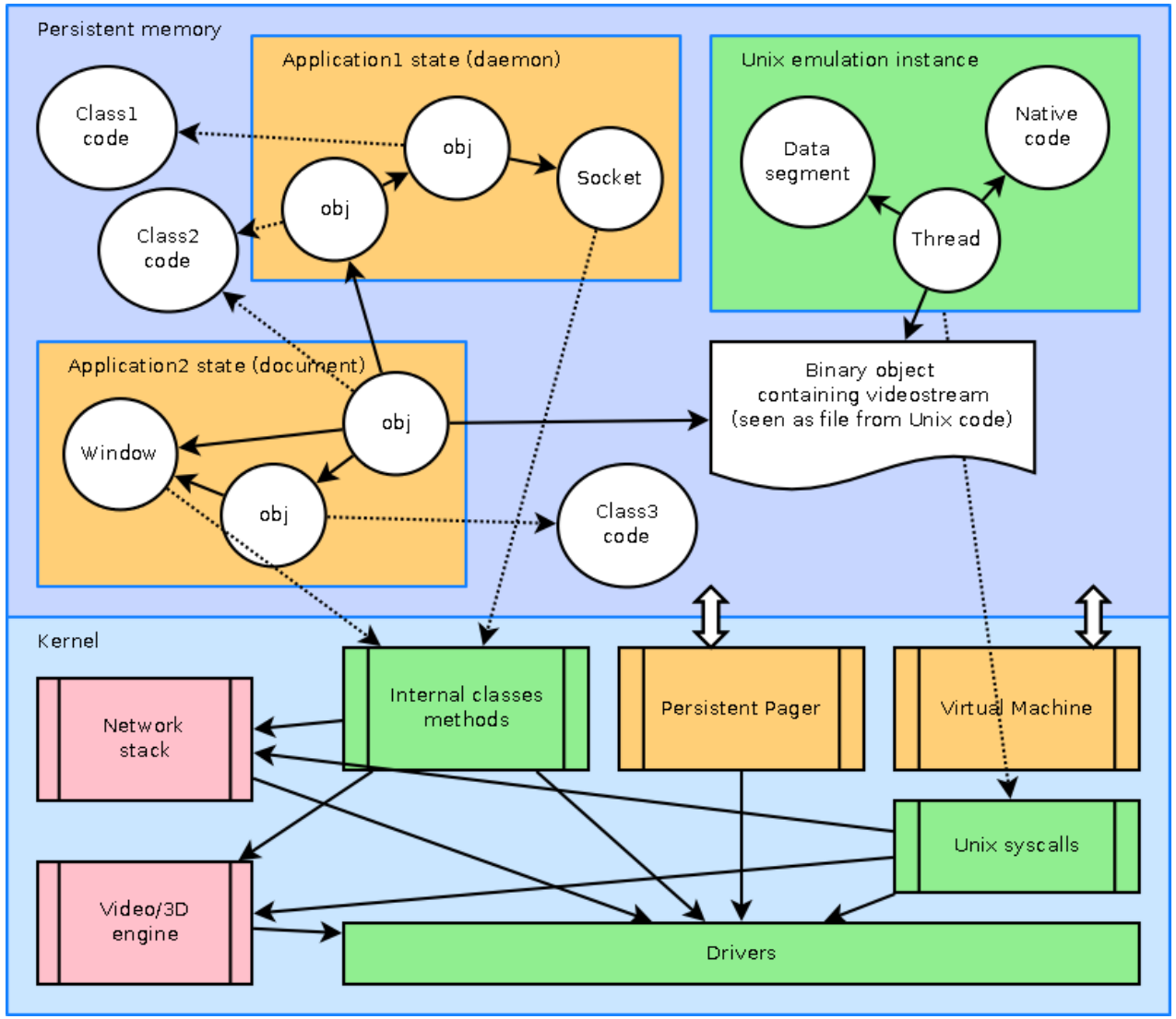
19

PHANTOM



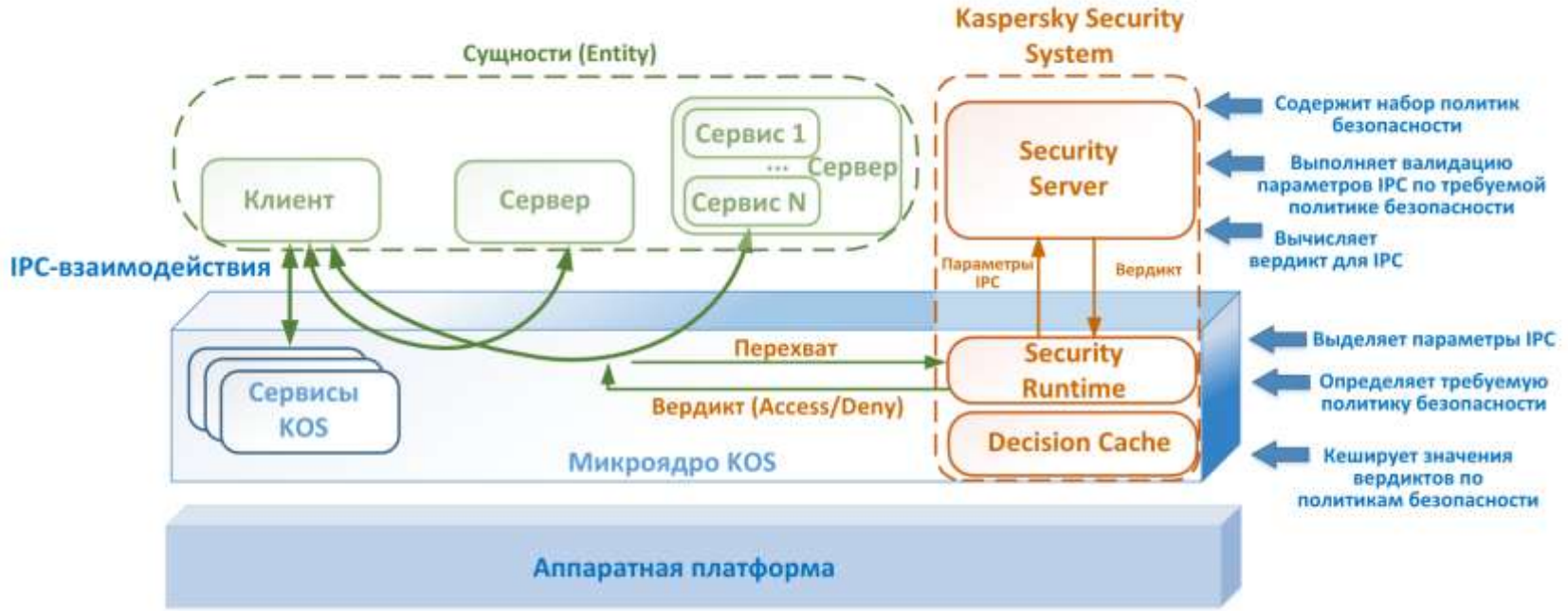
Операционная система **Phantom** базируется на концепции персистентной виртуальной памяти

http://phantomos.org/



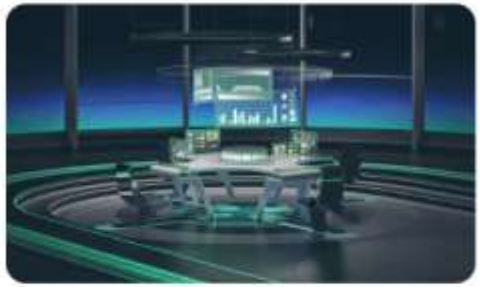
KASPERSKYOS

KasperskyOS – микроядерная операционная система, реализующая концепцию монитора обращений.
Решение на базе KasperskyOS состоит из изолированных *сущностей* (с ущность является аналогом процесса).
Сущности взаимодействуют друг с другом и с ядром посредством *интерфейсов*.
Интерфейсы, реализуемые сущностями, должны быть *статически описаны*.



Kaspersky IoT Infrastructure Security

Защита интернета вещей на уровне кибериммунных шлюзов



Kaspersky Secure Remote Workspace

Кибериммунная и функциональная инфраструктура тонких клиентов

Kaspersky Automotive Adaptive Platform

Построение надежных IT-систем для умного автотранспорта

https://os.kaspersky.ru/development/

ASTRA LINUX

29.11.2022г ГК «Астра» выпустила новую версию системы для управления доменом ALD Pro 1.2.0

Изменения коснулись наиболее востребованного функционала продукта: ролевой модели, позволяющей распределять права доступа между системными администраторами, заменены некоторые системные компоненты, обновлена сопроводительная и внутренняя документация

Теперь в ALD Pro есть дополнительные системные роли, позволяющие настроить решение более гибко в крупных компаниях. Компонент dnsmasq заменён на ISC DHCP для обеспечения более высокой отказоустойчивости DHCP-сервера — увеличено количество сетевых устройств, поддерживаемых одним…

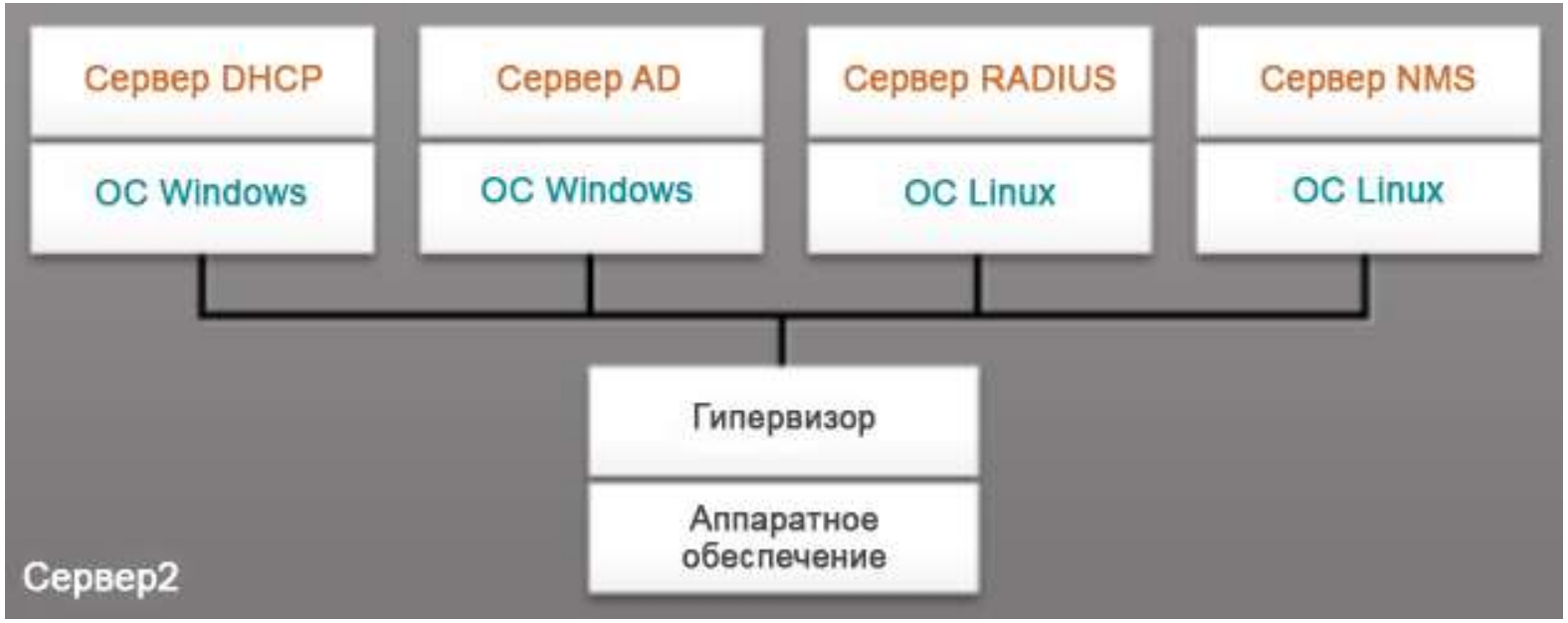
https://astralinux.ru/products/ald-pro

ВИРТУАЛИЗАЦИЯ

- Традиционно в организациях доступ к приложениям и службам организуется с применением мощных выделенных серверов.
- Это выделенные серверы с большим объемом ОЗУ, мощными процессорами и несколькими емкими устройствами хранения данных.
- К их недостаткам относятся неэффективное расходование ресурсов, единая точка отказа и расползание серверов.

ВИРТУАЛИЗАЦИЯ СЕРВЕРА

- Виртуализация серверов дает возможность использовать незадействованные ресурсы, чтобы сократить необходимое количество серверов.
- Программа **гипервизор** управляет ресурсами компьютера и ВМ.
- Она обеспечивает для ВМ доступ к аппаратным компонентам физического компьютера — ЦП, памяти, дисковым контроллерам и сетевым адаптерам.
- Каждая ВМ использует отдельную полнофункциональную операционную систему.



ВИРТУАЛИЗАЦИЯ КЛИЕНТА

- Виртуализация на стороне клиента дает пользователям возможность запускать ВМ на локальных компьютерах.
- Она обеспечивает пользователей ресурсами для тестирования новых операционных систем и программ и для работы с ранними версиями ПО.
- **Хост** — это физический компьютер под управлением пользователя.
- **ОС хоста** — это операционная система хост-компьютера.
- **Гостевая ОС** — это операционная система, работающая на ВМ.

ГИПЕРВИЗОРЫ

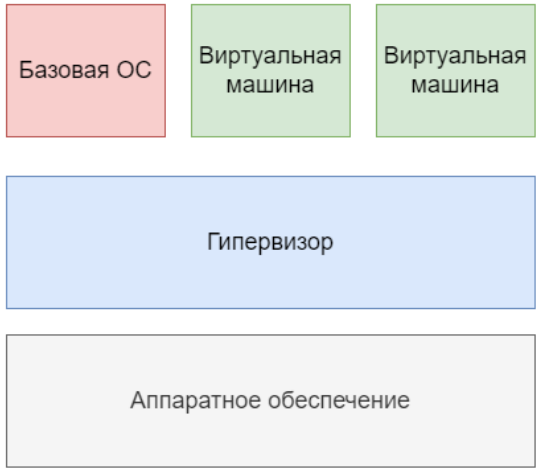
Гипервизоры первого типа (native, bare-metal)

Гипервизор первого типа выполняется как контрольная программа непосредственно на аппаратной части компьютера и не требует ОС общего назначения. В данной архитектуре гипервизор управляет распределением вычислительных ресурсов и сам контролирует все обращения виртуальных машин к устройствам.

Гипервизоры второго типа (hosted)

Гипервизор второго типа выполняется поверх хостовой операционной системы (как правило Linux). Он управляет гостевыми операционными системами, в то время как эмуляцией и управлением физическими ресурсами занимается хостовая ОС.

Гипервизоры гибридного типа (hybrid)



Гибридный гипервизор сочетает в себе характеристики гипервизоров первого и второго типов – он выполняется поверх специализированной сервисной (или базовой) операционной системы. Сервисная ОС называется родительским разделом или доменом (parent partition в терминологии Hyper-V или domain dom0 в терминологии Xen).

ВИРТУАЛИЗАЦИЯ

Требования, предъявляемые виртуальными машинами

Минимальные требования Windows Hyper-V для Windows 10	
ОС хоста	Windows 10 Pro или Windows Server (2012 и 2016)
Процессор	64-разрядный процессор с преобразованием адресов второго уровня (SLAT)
BIOS	Поддержка расширения VM Monitor Mode Extension (VT-c в ЦП Intel) центральным процессором
Память	Системное ОЗУ минимум 4 ГБ
Пространство на жестком диске	Минимум 15 ГБ на каждую ВМ

Hyper-V включен в Windows 10 Pro

ВИРТУАЛИЗАЦИЯ

Виртуализация – это сокрытие конкретной реализации за универсальным стандартизованным методом обращения к ресурсам. Иными словами, это создание абстракции над аппаратным обеспечением.

Существует много видов виртуализации, однако можно выделить три основных:

•**Аппаратная виртуализация.**
Позволяет создавать независимые и изолированные друг от друга виртуальные компьютеры с помощью программной имитации ресурсов (процессора, памяти, сети, диска и др.) физического сервера. Физический сервер называют хостовой машиной (хостом), виртуальные компьютеры – **виртуальными машинами**, ВМ (иногда их также называют гостями). Программное обеспечение, которое создает виртуальные машины и управляет ими, называют гипервизором (а также виртуальным монитором или контрольной программой). На практике на виртуальных машинах могут использоваться разные ОС для разных целей – например, Windows Server под контроллер домена Active Directory и Debian под веб-сервер NGINX.

•**Виртуализация рабочих столов**.
Позволяет отделить **логический рабочий стол** (набор пользовательских программ, работающий под ОС) от физической инфраструктуры (например, персональных компьютеров). Одной из наиболее распространенных форм виртуализации рабочих столов является VDI (Virtual Desktop Infrastructure) – инфраструктура виртуальных рабочих столов. Каждый пользователь VDI имеет программную имитацию ОС с необходимым набором программ на физическом сервере под управлением гипервизора и может подключаться к ней по сети. На практике VDI может использоваться для работы большого количества сотрудников на «удаленке» для того, чтобы не закупать им отдельные рабочии станции и управлять инфраструктурой централизованно.

•**Виртуализация на уровне ОС** (контейнеризация).
Позволяет запускать программное обеспечение в изолированных на уровне операционной системы пространствах. Наиболее распространенной формой виртуализации на уровне ОС являются контейнеры (например, Docker). Контейнеры более легковесны, чем виртуальные машины, так как они опираются на функционал ядра ОС и им не требуется взаимодействовать с аппаратным обеспечением. На практике контейнеры представляют из себя изолированную среду для запуска любого приложения со всеми его зависимостями и настройками.

ВИРТУАЛИЗАЦИЯ

Методы и функции, которые предоставляет виртуализация, могут оказаться весьма полезными в следующих случаях.

■■ Запуск пользовательских приложений, созданных для других операционных систем без перезагрузки компьютера.

■■ Запуск сетевых служб, созданных для других операционных систем без перезагрузки компьютера.

■■ Тестирование программного обеспечения, созданного программистом для других операционных систем.

■■ Изучение сетевого взаимодействия с помощью единственного компьютера.

■■ Изучение различных операционных систем. Преимущества использования виртуальных машин при

изучении операционных систем.

■■ Возможность установить операционную систему без изменения структуры разделов физического жесткого диска – на виртуальном диске, который является обычным файлом в файловой системе компьютера.

Часть 2

1. Модели информационной безопасности
2. Риски и угрозы, их реализация
3. Нормативные документы в области информационной безопасности
4. Инструменты безопасности