Организационно-техническая защита информации

М.Г. Лагутин

Информация

Конфиденциальность

Целостность

Доступность

Оборудование

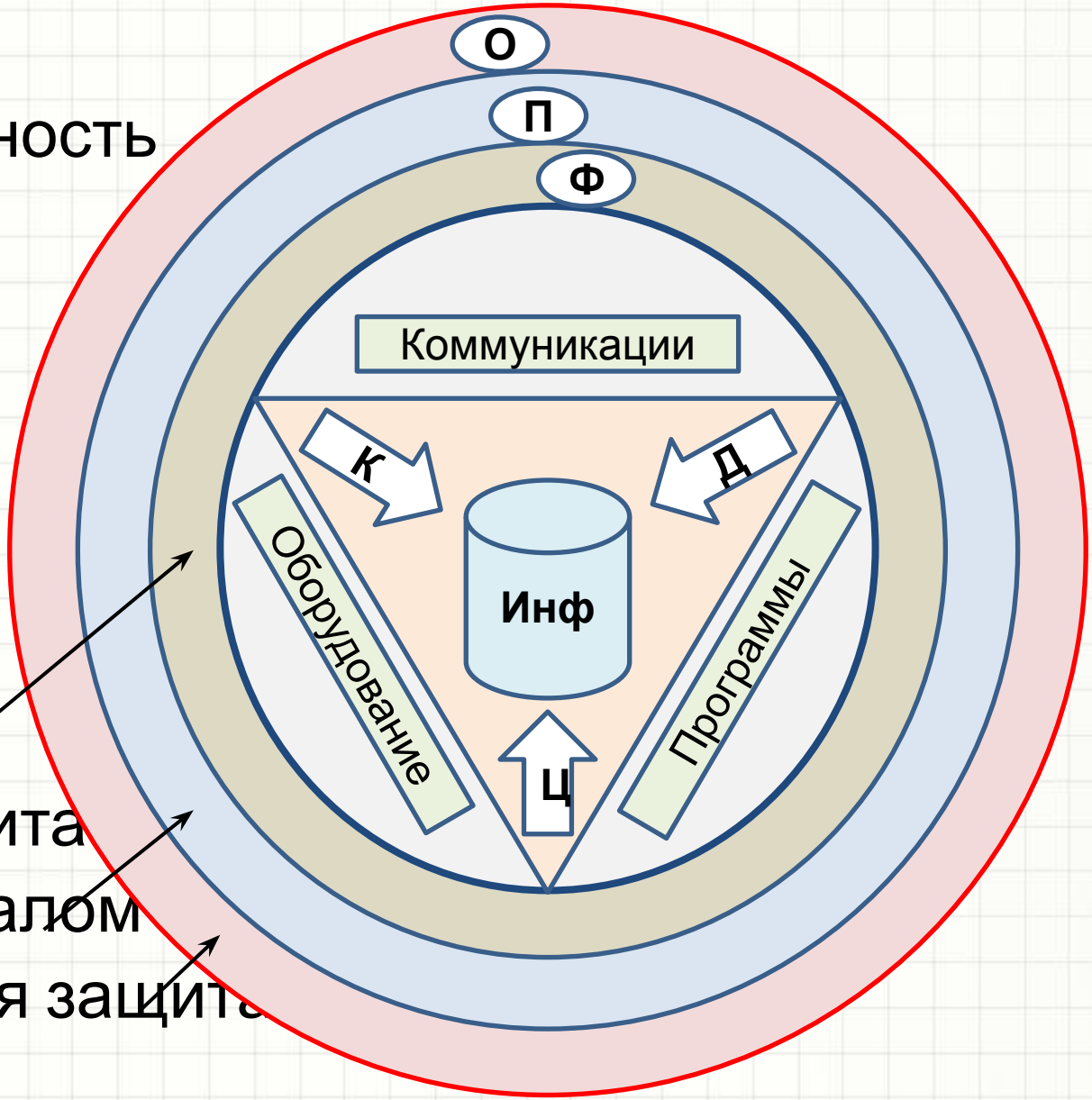
Программы

Коммуникации

Физическая защита

Работа с персоналом

Организационная защита



Направления орг.-технич.ЗИ на ОИ

1. Определение состава и назначения ОИ.
2. Физическая защита объекта.
3. Инженерное обеспечение объекта.
4. Организ.защита – кадровое обеспечение:

- назначение ответственных лиц;
- определение порядка доступа к ОИ, ПРД;
- обучение пользователей;
- закрепление ответственности допущенных лиц;
- обеспечение контроля и управления доступом

Направления орг.-технич.ЗИ на ОИ

5. Технические меры защиты (установка и настройка оборудования и/или ПО для ЗИ):

- доверенная загрузка (BIOS, иные носители);
- средства идентификации пользователей;
- использование лицензионных ОС и прикл. ПО;
- ограничение на использ. внешних носителей;
- шифрование;
- антивирусная защита (контроль и обновления);
- межсетевое экранирование.

Начальная загрузка

- Инициализация ЦП и устройств BIOS.
- Самотестирование устройств (POST).
- Опрос загрузочных устройств и передача управления на выбранное загр.устройство.

Сокращённый тест POST включает:

Проверку целостности программ BIOS в ПЗУ, используя контрольную сумму.

Обнаружение и инициализацию основных контроллеров, системных шин и подключенных устройств и выполнение программ инициализации этих устройств.

Определение размера оперативной памяти и тестирования первого сегмента (64 килобайт).

POST (power on self test)

Полный регламент работы POST:

- Проверка регистров процессора;
- Проверка контрольной суммы ПЗУ;
- Проверка системного таймера и порта звуковой сигнализации;
- Тест контроллера прямого доступа к памяти;
- Тест регенератора оперативной памяти;
- Тест нижней области ОЗУ для проецирования резидентных программ в BIOS;
- Загрузка резидентных программ;
- Тест стандартного графического адаптера (VGA);

POST – полный набор

- Тест оперативной памяти;
- Тест основных устройств ввода (не манипуляторов);
- Тест CMOS;
- Тест основных портов LPT/COM/USB;
- Тест накопителей на жёстких магнитных дисках (НЖМД);
- Самодиагностика функциональных подсистем BIOS;
- Передача управления загрузочному устройству.

Иные варианты начальной загрузки

- по COM порту;
- по LPT порту;
- с использованием HPI (Host-Port Interface) - Cisco;
- загрузка после «горячей» перезагрузки.

Загрузочные устройства

Предварительно составленный список и закрепленная в BIOS последовательность опроса:

- Один/несколько жестких дисков;
- Устройство чтения CD/DVD;
- USB-устройства;
- Сетевая карта (загрузка по PXE).

Загрузка всегда передается на нулевой сектор загр. устройства, где размещается загрузчик ОС (особый случай – HDD).

Загрузка с жесткого диска

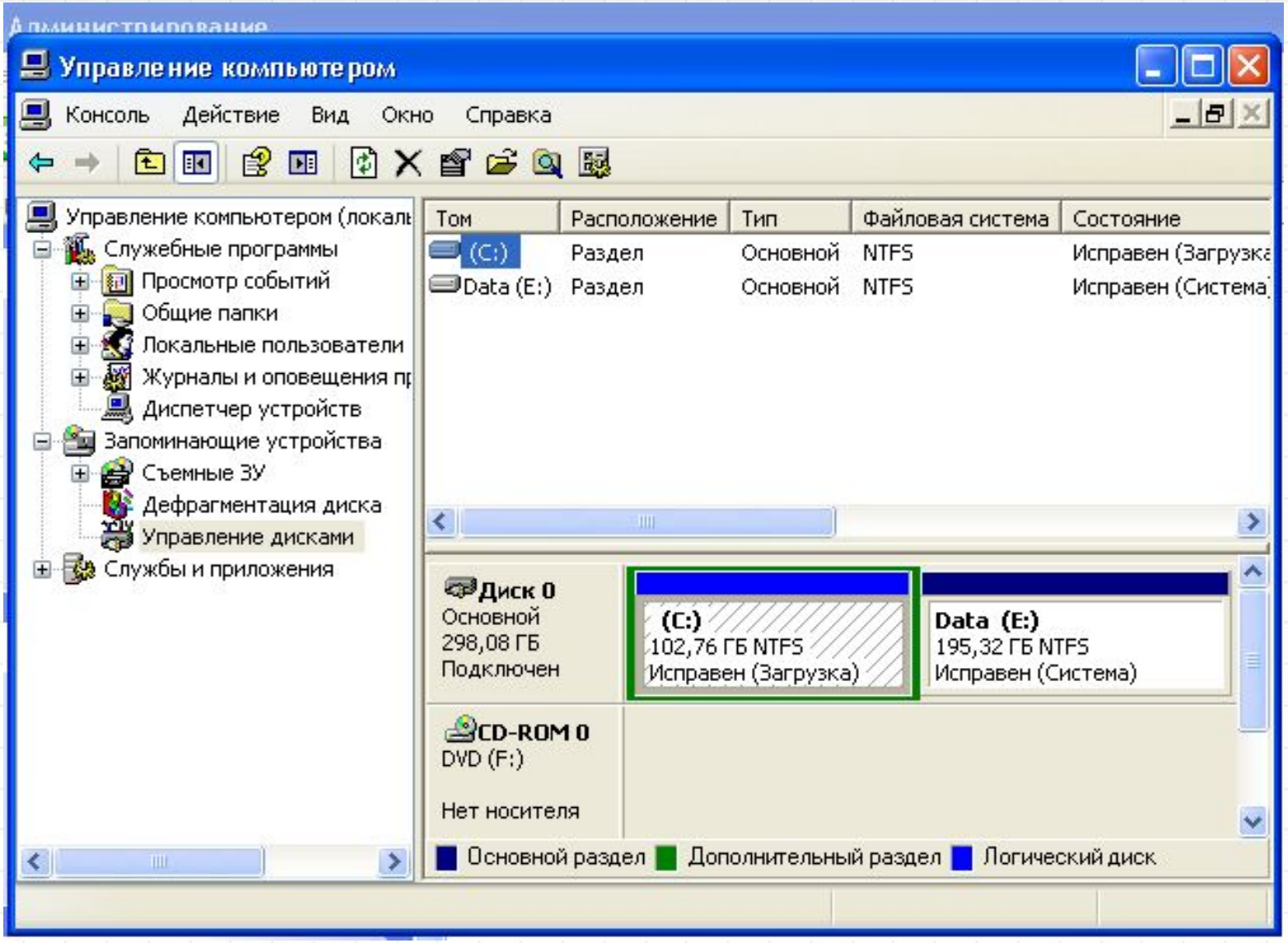
Может иметь логическое деление на разделы. Раздел м.б. активным

Главная загрузочная запись (MBR):

- расположена в 0 секторе НЖМД;
- не зависит от ОС;
- содержит управляющий код, таблицу разделов и указатель перехода на boot sector акт.раздела.

Основная задача – найти активный (и доступный) раздел и передать управление загрузчику ОС.

Логическое разбиение



Загрузчик ОС

Задачи загрузчика ОС:

- диалог с пользователем (выбор ОС);
- настроить устройств BIOS для загрузки ядра ОС;
- загрузить ядро ОС в ОЗУ;
- настроить окружение;
- передать управление ядру ОС.

В момент загрузки ядра происходит переключение в 32-х или 64-хбитный режим адресации памяти.

Ядро Windows NT-200x

исполняющая система NT, которая включает управление памятью, процессами, потоками, безопасностью, вводом/выводом, межпроцессорными обменами;

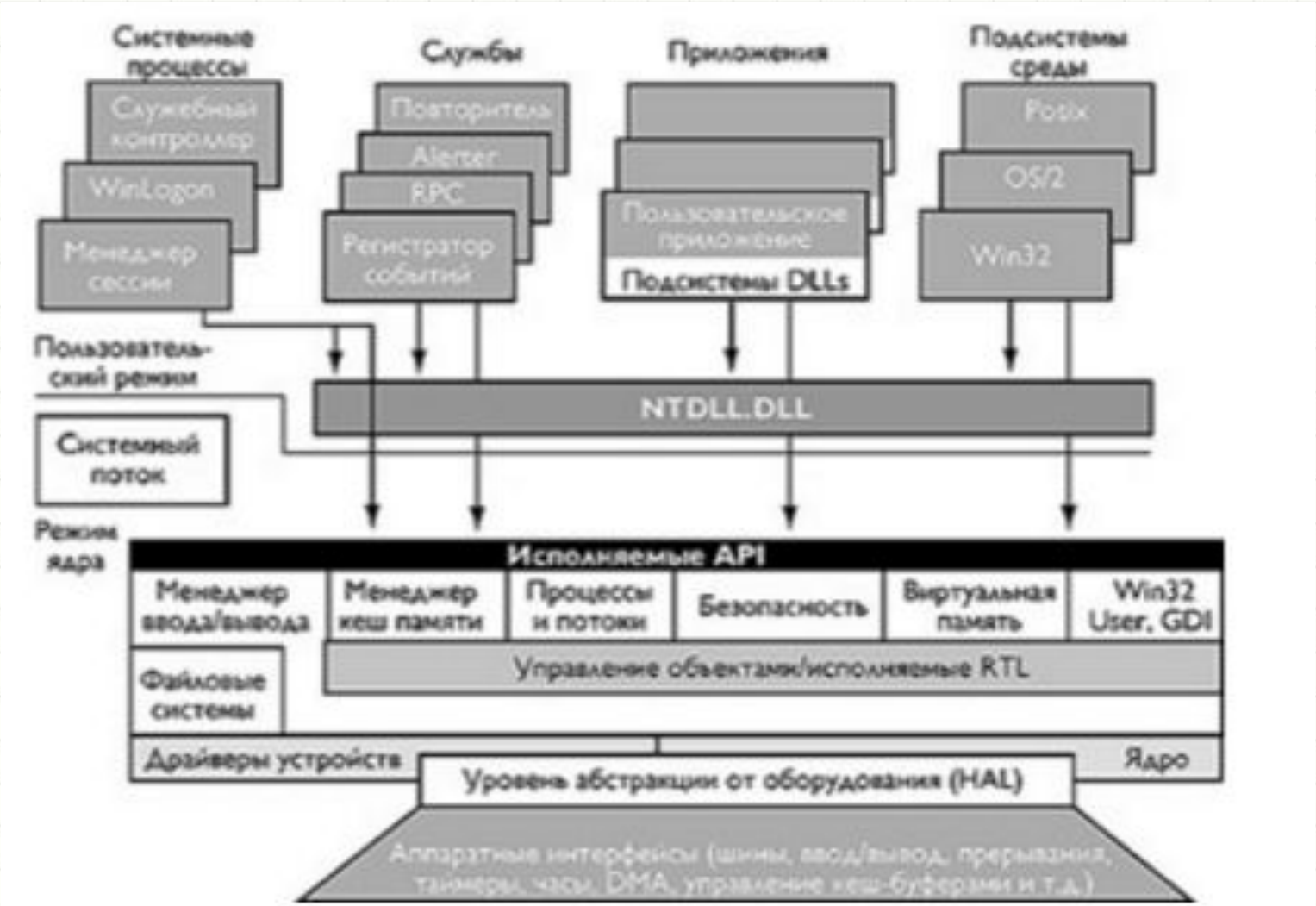
ядро (микроядро) Windows NT выполняет низкоуровневые функции ОС: диспетчеризация потоков, прерываний и исключений, синхронизация процессоров. Ядро также включает набор процедур и базовых объектов, используемый исполняемой частью для создания высокоуровневых конструкций;

уровень абстракции от оборудования (HAL – Hardware Abstraction Layer), изолирует ядро, драйверы устройств и исполняемую часть NT от аппаратных платформ, на которых должна работать ОС. Подобный подход позволяет обеспечить переносимость Windows NT.

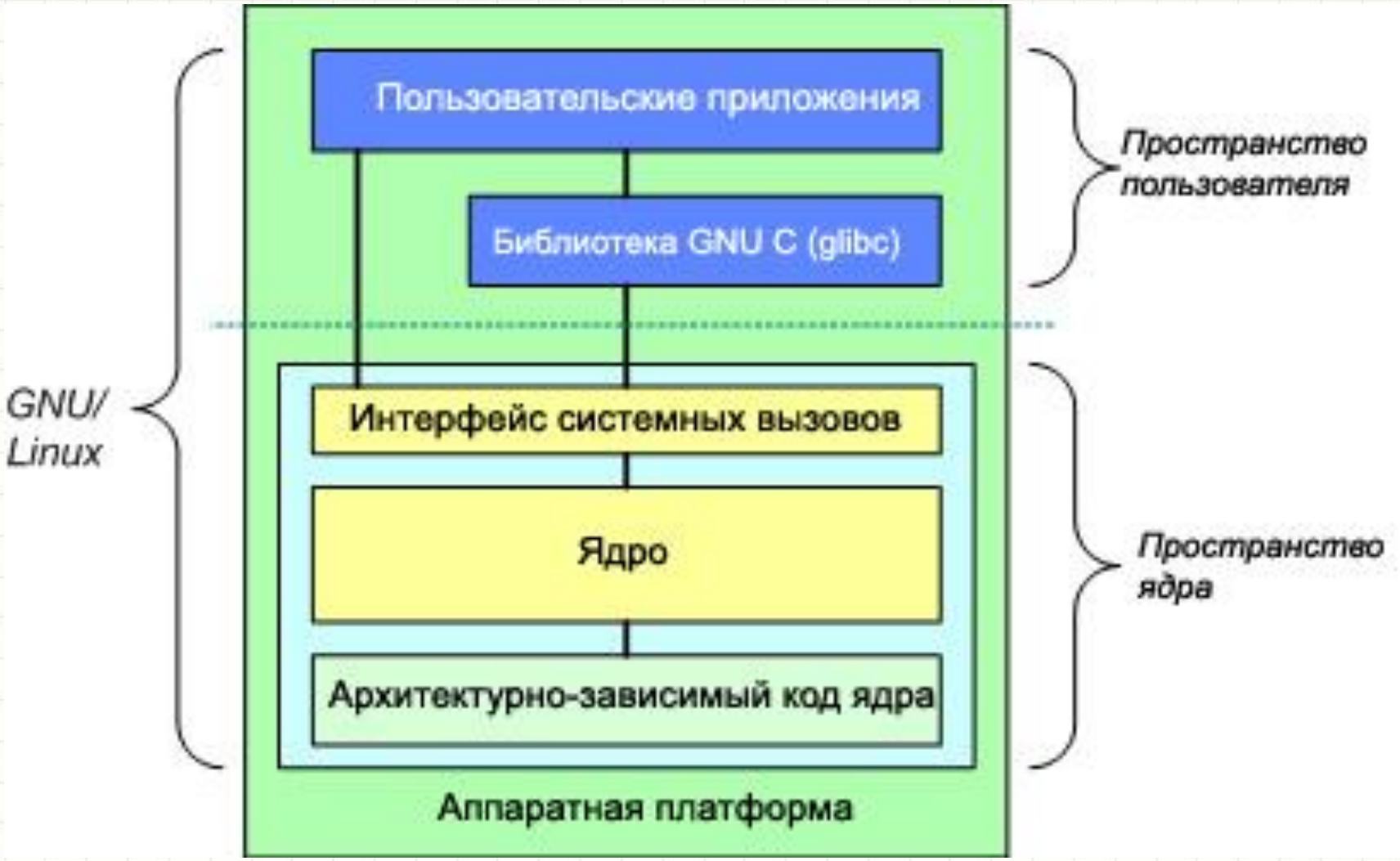
драйверы устройств включают как файловую систему, так и аппаратные драйверы, которые транслируют пользовательские вызовы функций ввода/вывода в запросы физических устройств ввода/вывода;

функции графического интерфейса пользователя работают с окнами, элементами управления и рисунками.

Архитектура Windows NT-200x



Ядро Linux


Пользовательские приложения
Библиотека GNU C (glibc)
Интерфейс системных вызовов
Ядро
Архитектурно-зависимый код ядра
Аппаратная платформа
GNU/ Linux
Пространство пользователя
Пространство ядра

Особенности выполнения ядра ОС

- Имеет отдельные, но тесно взаимосвязанные модули-подсистемы.
- Никогда не выгружается из ОЗУ.
- Выполняется в защищенном режиме (кольца защиты – изучить самостоятельно).
- Скрывает от прикладного ПО конкретную аппаратную реализацию.

Доверенная загрузка

загрузка различных операционных систем только с заранее определенных постоянных носителей после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации / аутентификации пользователя.

Цепочка доверенной загрузки – последовательная передача процедуры загрузки по набору разрешенных устройств.

Варианты доверенной загрузки

- Пароль BIOS на загрузку компьютера и визуальный осмотр целостности защитных наклеек на корпусе ПК до включения.
- Спец.прошивка BIOS (ограничения по объему кода в ПЗУ материнской платы).
- Спец.загрузочный носитель (CD/DVD/USB-flash).
- Использование спец.ПО для шифрования дисков или отдельных областей (PGP Tools).
- Использование аппаратно-программных средств доверенной загрузки.

Аппаратно-программные средства

- Аппаратный модуль доверенной загрузки «Аккорд-АМДЗ».
- Модуль доверенной загрузки «Криптон-замок/PCI».
- Электронный замок «Соболь».

Преимущества – собственная аппаратная часть, прошивка и область хранения данных, перехват управления до начала работы BIOS.

При шифровании области диска изъятие устройства гарантирует невозможность считывания данных.

Основные функции

- функции идентификации/аутентификации пользователей (несколько стадий);
- контроль целостности аппаратной и программной среды (тест, контрольные суммы, шифрование);
- администрирование и аудит.

Электронный замок «Соболь».

Сертификат ФСТЭК России 1967 RU.40308570.501410.001 использование в АС, обрабатывающих сведения до сс

Модель	Спецификация
	• Габариты: 50 x 120 мм. • Интерфейс: PCI (3,3 В, 5 В). • Разъем RJ12 для подключения внешнего считывателя идентификатора iButton. • Разъем для подключения внутреннего считывателя идентификатора iButton. • Соединительный кабель для механизма сторожевого таймера. • Упаковка: индивидуальная. **Поддерживаемые идентификаторы:** • iButton DS1992, DS1995 и DS1996. • USB-ключи iKey 2032. • USB-ключи eToken PRO. • USB-ключи eToken PRO (Java). • Смарт-карты eToken PRO через USB-считыватель Athena ASEDrive IIIe USB V2 . • USB-ключи Rutoken, Rutoken RF.

Функциональные возможности

- Идентификация и аутентификация пользователей до запуска BIOS;
- Блокировка загрузки операционных систем со съемных носителей;
- Контроль целостности программной среды;
- Контроль целостности системного реестра Windows;
- Контроль конфигурации компьютера (PCI-устройств, ACPI, SMBIOS);
- Сторожевой таймер и датчик случайных чисел;
- Регистрация попыток доступа к ПЭВМ;
- Программная инициализация и контроль конфигурации комплекса;
- Поддержка высокоскоростного режима USB 2.0/3.0;
- Поддерживаемые файловые системы: NTFS5, NTFS, FAT 32, FAT 16, FAT 12, UFS, UFS2, EXT3, EXT2, EXT4.

Пример

1. Какие из организационных документов уже д. б.?

2. Действия администратора ИБ при настройке УДЗ.

- АС тип 1
- СУБД (гриф сс)
- 5 польз.(ИБ,БД, 3 простых)
- Дов.загрузка «Соболь» …

Определить загр.устройства.

Снять контрольные суммы.

Создать профили пользователей.

Определить критичные события и реакцию на них.

Документы на объекты информатизации (ОИ):

перечень помещений, в которых проводятся секретные мероприятия, технических средств и систем, используемых для обработки информации, содержащей государственную тайну;

распоряжение о назначении комиссии по категорированию, классификации и организации аттестации объекта информатизации;

акты категорирования ОИ;

предписание на основные технические средства и системы (ОТСС) объектов вычислительной техники (ОВТ) и протокол специальных исследований;

предписание на ОТСС и вспомогательные технические средства и системы (ВТСС), установленные в выделенных помещениях (ВП), с протоколами специальных исследований;

заключение по результатам специальной проверки технических средств и систем ОИ;

схема расположения ОИ с привязкой к границам контролируемой зоны (КЗ) (указываются расстояния);

схемы размещения ОТСС, ВТСС и средств защиты информации (СЗИ) на ОИ, прокладка линий связи, сигнализации и коммуникаций; схемы электропитания и заземления ОВТ;

протоколы измерения параметров заземляющего устройства ОТСС и ВТСС;

технические паспорта на ОИ;

акты классификации автоматизированных систем (АС);

список лиц, обслуживающих ОИ;

список лиц, имеющих доступ в помещение с ОИ;

список лиц, допущенных к самостоятельной работе на ОИ;

список лиц, имеющих доступ в ВП;

перечень используемых в АС программных средств;

описание технологического процесса обработки информации в АС;

перечень защищаемых ресурсов в АС;

матрица разграничения доступа к информационным ресурсам АС в составе ОИ;

распоряжение о назначении уполномоченного (администратора) по защите информации из числа сотрудников, допущенных к обработке информации;

технологическая инструкция администратору безопасности объекта информатизации;

технологические инструкции пользователям АС по обеспечению защиты информации при обработке сведений, содержащих государственную тайну; инструкция пользователю по антивирусной защите АС; акт установки систем защиты;

документация на комплекс средств защиты;

сертификаты (копии) на установленные средства защиты информации;

инструкция (памятка) по обеспечению защиты секретной информации;

данные по уровню подготовки кадров, обеспечивающих защиту информации на ОИ;

заявка на проведение аттестации ОИ;

приказ о вводе в эксплуатацию ОИ;

программа и методика проведения аттестационных испытаний ОИ;

заключение по результатам аттестационных испытаний ОИ;

аттестат соответствия ОИ требованиям безопасности информации;

Вредоносное ПО.

Компьютерный вирус - это специально написанная небольшая по размерам программа, имеющая специфический алгоритм, направленный на тиражирование копии программы или её модификацию и выполнению действий, нарушающих ИБ автоматизированной системы.

Типичные варианты попадания в систему: съемные носители (USB-CD-DVD), по сети (эл. почта, ICQ-Wiber etc, вход пользователя на опасные ресурсы).

Признаки заражения

- ОС или прикладные программы перестают работать или начинают работать некорректно.
- На экран выводятся посторонние сообщения, сигналы и другие эффекты.
- Работа компьютера существенно замедляется.
- Структура некоторых файлов и каталогов оказывается испорченной.

Классификация вирусов

1. По месту «жительства», среде распространения:

- Загрузочные (boot sector загрузочных устройств).
- Файловые (файлы исполняемых модулей, конфигурационные файлы, файлы с текстом исполняемых команд).
- Сетевые (используют особенности сетевых протоколов).

2. По способу заражения:

- Резидентные (размещают модуль в ОЗУ).
- Нерезидентные

Классификация вирусов

3. По особенностям алгоритмов:

- паразитические («съедают» ресурсы),
- репликаторы (черви),
- невидимки (резиденты, перехват прерываний и выдача «чистого» файла),
- мутанты (полиморфы, самомодифицируются),
- троянские (маскировка под др.программы),
- логические бомбы (по наступлении события),
- макро-вирусы.

4. По тяжести последствий.

Методы предупреждения

- Личные знания и ответственность.
- Внимание при любых действиях в сети или с использованием недоверенных носителей.
- Регулярный контроль и аудит.
- Резервное копирование.
- Соблюдение установленных правил ИБ: правила разграничения доступа, правила реагирования на предполагаемое заражение и т.д.

Варианты борьбы с вирусами

- Врукопашную, с использованием файловых менеджеров и стандартных утилит ОС. Четкое знание элементов автозагрузки и их контроль, умение обнаружить следы действия вируса, вернуть правильные атрибуты файлов и каталогов.
- С использованием бесплатных утилит (проект cureit DrWeb'a) и Интернет-ресурсов http://www.virustotal.com
- Антивирусные программы.

Обзор антивирусов

1. Узкоспециализированное ПО (анти-autorun, антиспам, разблокировщики реклам).
2. Файловый антивирус.
3. ПО комплексной защиты.

- Детекторы (обнаружение заражения).
- Доктора (фаги, возврат программ в незараженное состояние).
- Ревизоры (сравнение с «идеальным» состоянием).
- Мониторы (резидентно, контроль изменений и отработка по правилам или выбору пользователя).

Распространенные производители

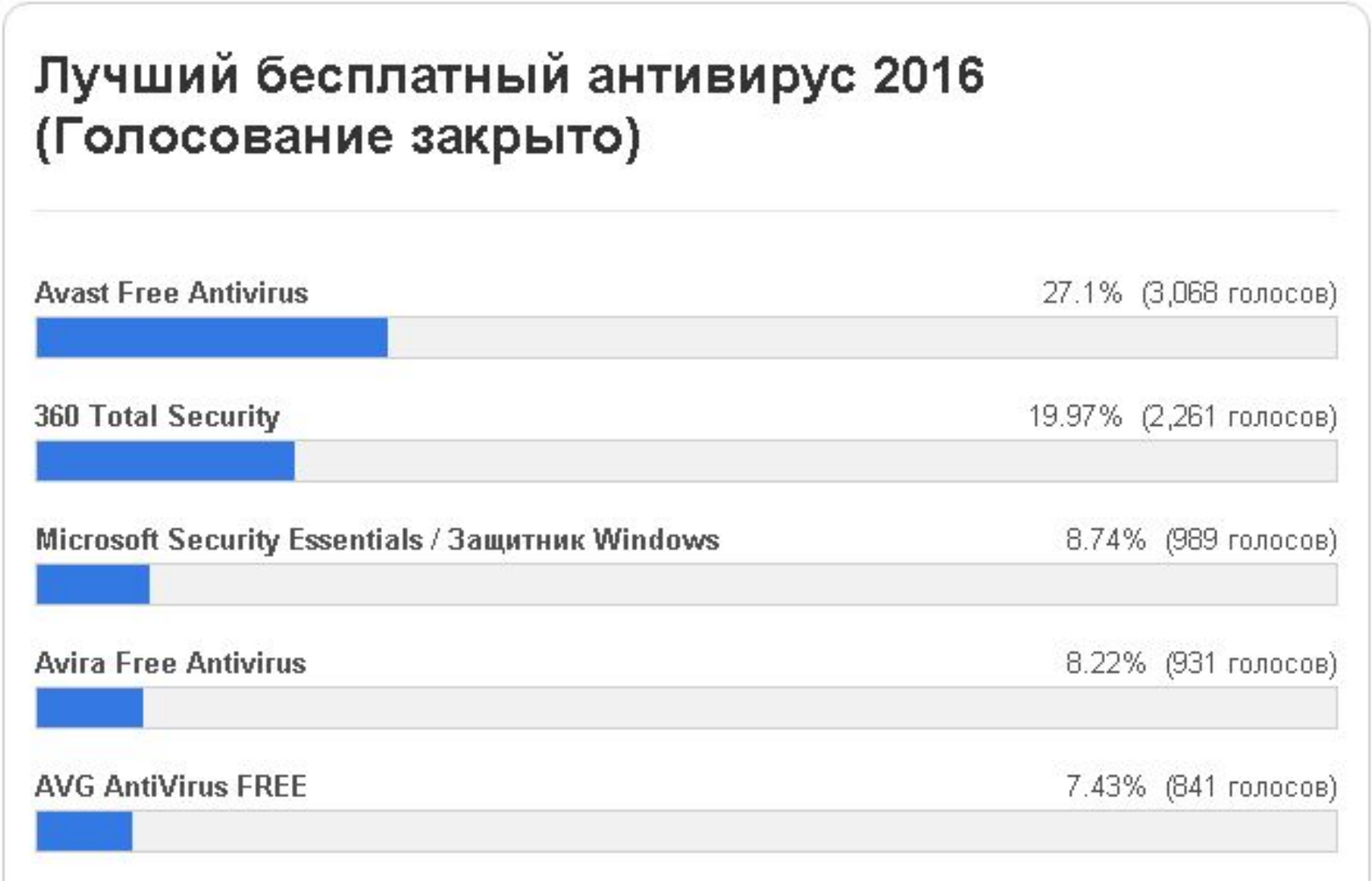
- ООО Доктор Веб (DrWeb), ранее Лаборатория Данилова, ДиалогНаука.
- Лаборатория Касперского (AVP).
- NOD32 (Eset, Словакия).
- Norton AntiVirus (Symantec, США).

Проблема выбора АВ для ОИ

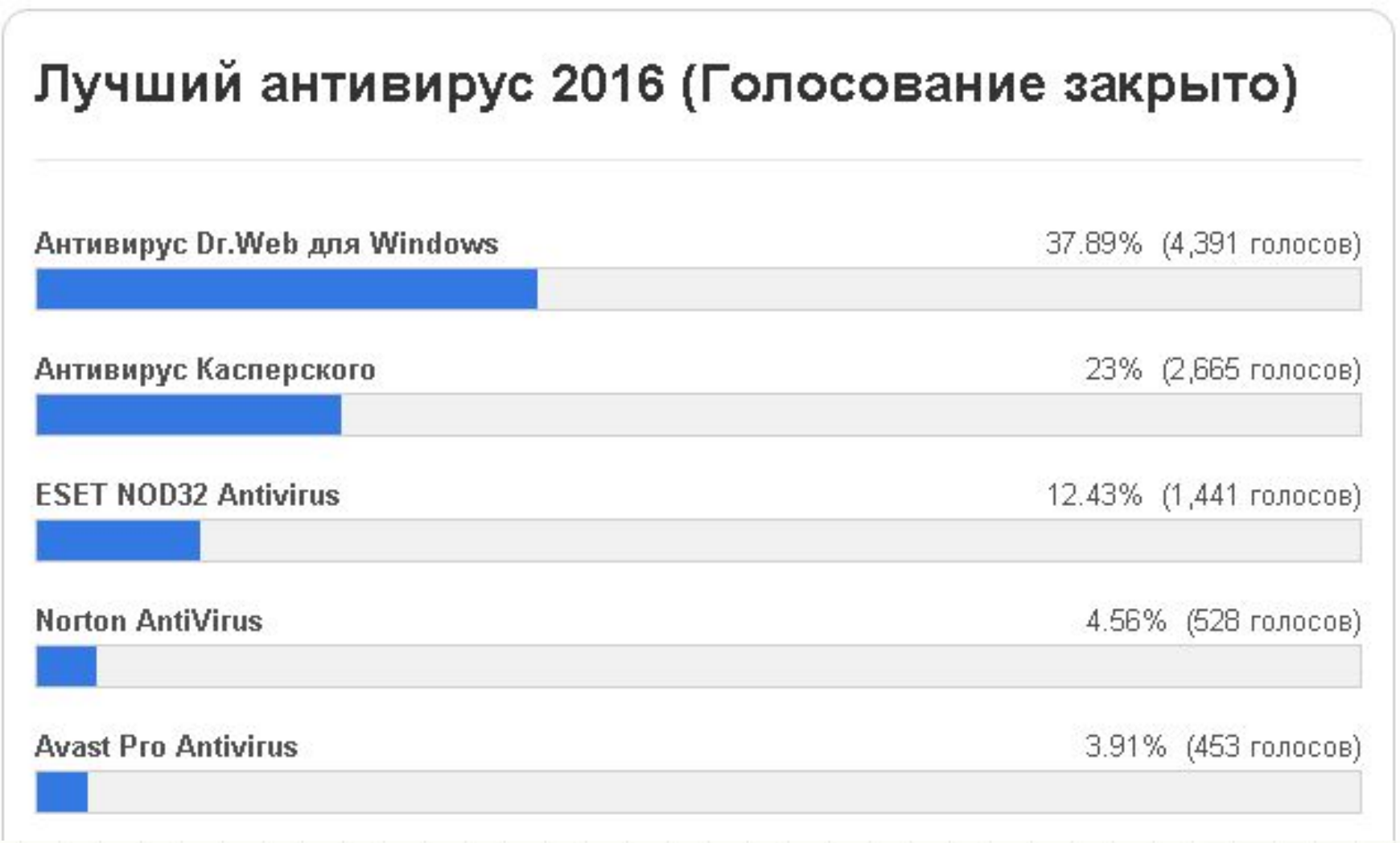
Необходимо ответить на вопросы:

- Насколько автономна ИС?
- Какие модули комплекса защиты необходимы?
- Технические характеристики АРМ и серверов.
- Критичность прерывания нормального функционирования ОИ.

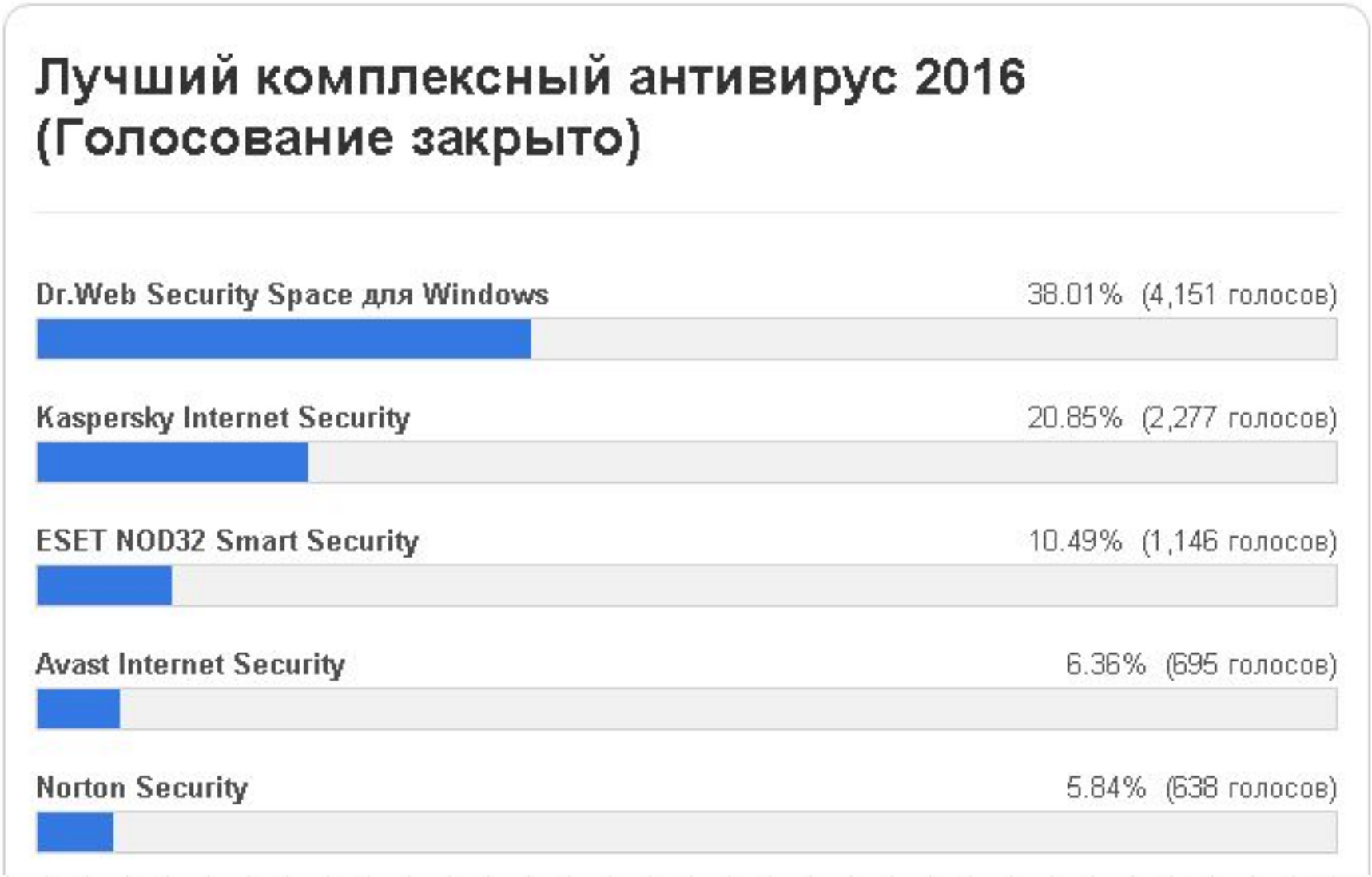
Рейтинги. http://www.comss.ru/



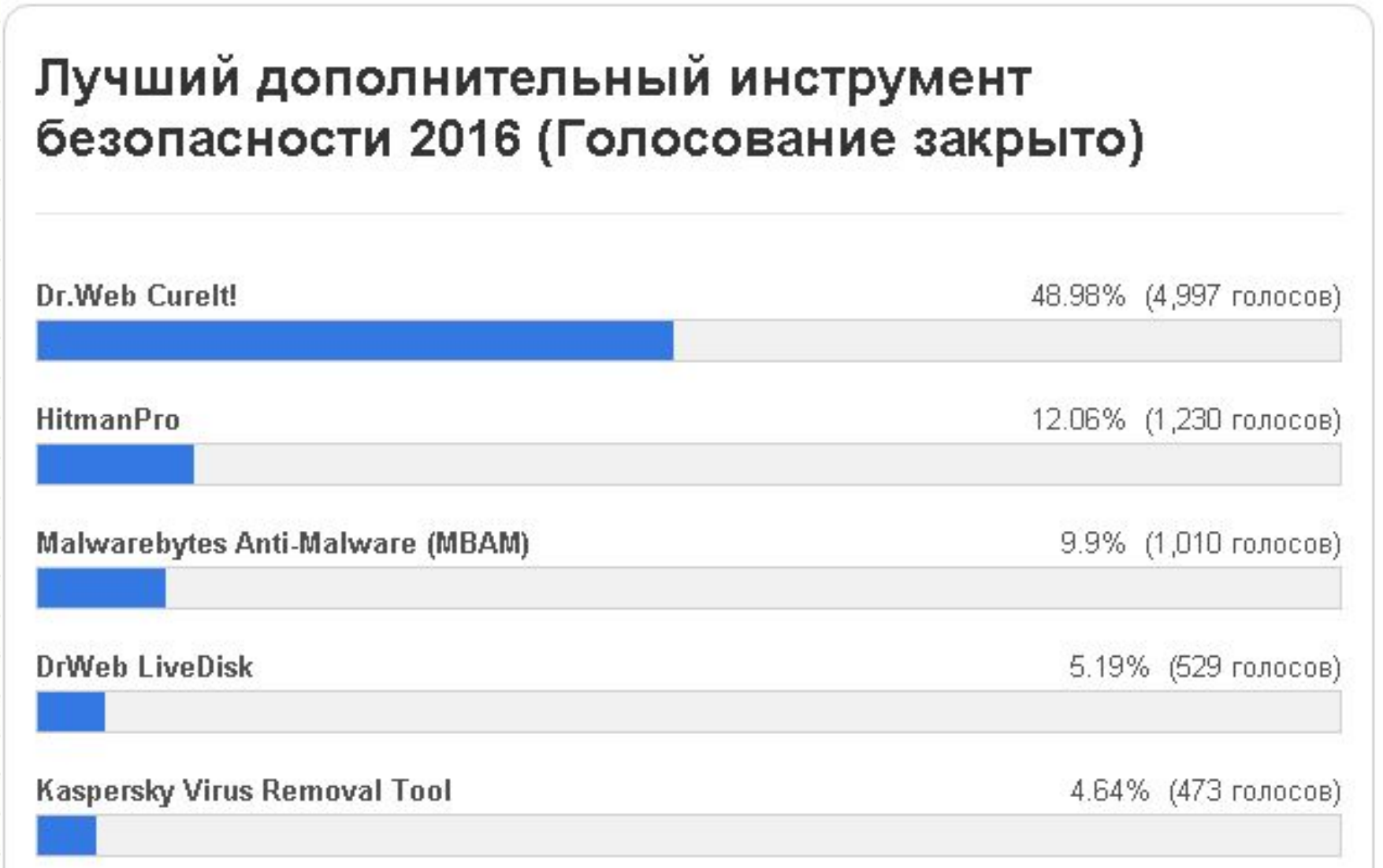
Рейтинги. http://www.comss.ru/



Рейтинги. http://www.comss.ru/



Рейтинги. http://www.comss.ru/



Вариант трудоустройства

Вакансия: Вирусный аналитик-стажер / Junior Malware Analyst в ООО «Доктор Веб».

Обязанности:

Анализ кода и функциональности вредоносного объекта;

Добавление записей о вредоносном объекте в антивирусные базы.

Требования:

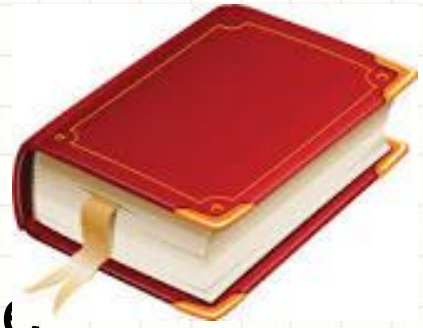
Знание Assembler x86;

Базовое владение инструментами OllyDBG, Hiew, IDA;

Базовые знание архитектуры Windows, PE-файлов;

Технический английский.

Должностная инструкция



формализованный документ, в котором закрепляются обязанности, ответственность и права сотрудника, предъявляемые к нему квалификационные требования.

Разрабатывается отделом кадров и/или руководителем подразделения, утверждается руководителем предприятия.

Структура должностной инструкции

- Общие положения.
- Квалификационные требования.
- Должностные обязанности.
- Ответственность.
- Права.

Пример – файл Word.

Задания на самостоятельную работу

Доклады на 31.03.2016

Кольца защиты

Проверочная работа

На 0,5 тетрадного листа Фамилия Имя

Группа и Дата

- Отношение к вакансии Вирусный аналитик-стажер в ООО Доктор Веб.
- Последовательность начальной загрузки (вплоть до передачи управления ядру ОС).
- Классификация вирусов по

  а). способу заражения

  б). среде распространения.

Вопросы?