# СОФИЙСКА ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ЕЛЕКТРОНИКА

**„ДЖОН АТАНАСОВ“**

# гр. София, ул. “Райко Алексиев“ № 48, email: [spgelectron@yahoo.co.uk,](mailto:spgelectron@yahoo.co.uk) spge-bg.com

**ДЪРЖАВЕН ИЗПИТ ЗА ПРИДОБИВАНЕ НА ТРЕТА СТЕПЕН НА ПРОФЕСИОНАЛНА КВАЛИФИКАЦИЯ**

**по професията код** 523050 „Техник на компютърни системи“

**по специалността код** 5230501 „Компютърна техника и технологии“

# ТЕМА: ВЪНШНИ ЗАПОМНЯЩИ УСТРОЙСТВА В СЪРВЪРНИ КОНФИГУРАЦИИ. ИЗГРАЖДАНЕ НА СЪРВЪР ПОД WINDOWS, СОФТУЕРЕН RAID МАСИВ. СЪВРЕМЕННИ ТЕХНОЛОГИИ ЗА АРХИВИРАНЕ НА ДАННИТЕ.

**МЕТОДИ ЗА ЗАЩИТА НА СЪРВЪРА, АРХИВА И МРЕЖАТА.**

# ИЗГОТВИЛ: ПЕТЪР ЯНКОВ ГЕРДЖИКОВ УЧЕНИК ОТ 12„Г“ КЛАС

**Дипломант:**

*/Петър Герджиков/*

# Ръководител:

***/****инж. Цветана Пунева/*

# СЪДЪРЖАНИЕ

УВОД стр. 3

I. ПЪРВА ЧАСТ…...…………………………………………………………………… стр. 5-13 ЗАПОМНЯЩИ УСТРОЙСТВА В СЪРВЪРНИ КОНФИГУРАЦИИ...……………………......

1. Флопи диск/FDD...………………………………………………………………………. стр. 5

2. Твърд диск/HDD…..…………………………………….………………………………. стр. 5

3. Солид стейт драйв/SSD…….…………………………………………………………… стр. 9

4. Оптични дискови устройства…………………….…………………………………… стр. 11 II. ВТОРА ЧАСТ…….……………………………….………………………………...стр. 14-22 СЪРВЪРИ – СЪЩНОСТ, ХАРАКТЕРИСТИКИ И КЛАСИФИКАЦИЯ. RAID МАСИВИ…. 1. Сървър/Server…………………………………………………………………..………. стр. 14 2. Конфигуриране на дискове……………………………………………………….……стр. 19 3. RAID масиви…………………………………………………………………………….стр. 20 III. ТРЕТА ЧАСТ……………………………………………………………………….стр. 23-35 ЗАПЛАХИ И МЕТОДИ ЗА ЗАЩИТА НА СЪРВЪРА……………………………………........

1. Заплахи за сигурността на сървъра…………………………………………………….стр. 23 2. Мерки за защита……………………………………………………………………...…стр. 25 3. Защитна стена/Firewall………………………………………………………………….стр. 25

4. Антивирусен софтуер/Antivirus software...……………………………………………стр. 27 5. Криптиране/Encryption…………………………………………………………...……. стр. 28 6. Бекъп/Backup……………………………………………………………………………стр. 31 7. Архивиране/Data archiving……………………………………………………………..стр. 34 IV. ЧЕТВЪРТА ЧАСТ…………………………………………………………………стр. 36-40 ПРАКТИЧЕСКА ПОСТАНОВКА……………………………………………………………….

1. Изграждане на сървър под операционна среда Windows Server 2019……………….стр. 36
2. Изграждане на софтуерен RAID масив под Windows Server 2019…………………..стр. 37 ИЗВОДИ, ОБОБЩЕНИЕ И ЗАКЛЮЧЕНИЕ……………………………………………стр. 40 ИЗТОЧНИЦИ……………………………………………………………………………….стр.42 ПРИЛОЖЕНИE……………………………………………………………………………стр. 44

# УВОД

* **Външното запомнящо устройство/ВЗУ** може да се определи като дигитален носител, използван с цел запис и съхранение на данни за дълъг период от време. Всички външни запомнящи устройства имат енергозависим принцип на запис.

Необходимостта от запазване на голямо количество информация за дълго време е наложило използването на ВЗУ.

# Разглеждайки развитието на външните запомнящи устройства през годините:

⁂ **Перфокартите** – са първият опит за запис на данни на машинен език. Представляват твърд хартиен носител на 80 байта информация. Съхраняват информацията, като я кодират чрез липсата или наличието на отвори на определени позиции (*фиг. 1 в приложение*). Използвали са се за прехвърляне на данни още преди компютрите да бъдат разработени. За записа на 1 GB информация на перфокарти е необходима голяма стая, а теглото ще бъде над 22 тона.

⁂ **Перфоленти** – това е дълга хартиена лента, в която са пробити дупки. Различава се от перфокартите по това, че лентата е непрекъсната. Перфокартите и веригите от перфокарти са се използвали за контрол на тъкачните машини през XVIII век (*препратка 1 в приложение*). Използването им за телеграфни системи започва през 1842 г. Перфорираната лента се използва

през 19-и и през по-голямата част от 20-и век за програмируеми тъкачни станове, за комуникация с телепринтер, за въвеждане в компютри през 50-те и 60-те години на 20-и век.

⁂ **Магнитни ленти** – те са тънко магнитно покритие върху дълга и тясна тънка пластмасова лента, едната повърхност на която е покрита с железен оксид, променящ свойствата си под въздействието на магнитно поле *(фиг. 2 в приложение*).

⁂ **Магнитни дискове** – представлява запомнящо устройство, което използва процес на намагнитване за запис, презапис и достъп до данни. Покрит е с магнитно покритие и съхранява данни под формата на писти, точки и сектори.

⁂ **Пакет магнитни дискове** – дисковите пакети и дисковите касети са били ранни форми на сменяеми носители за съхранение на компютърни данни, въведени през 60-те години на XX век.

⁂ **Голяма 3,5′′ дискета** – гъвкав диск, направен от пластмаса, покрит с тънък магнитен слой и

затворен в защитна опаковка.

⁂ **Дискета** – тя е направена от специална пластмаса с магнитно покритие и е поставена в пластмасова обложка. Има повърхности върху които се записват данни. Всяка повърхност има

зона за запис, малко по-тясна от един инч, която е разделена на пътеки, които се намират от **О**. Дискетата се върти с постоянна скорост при запис или четене, при което се движат главите.

* **Изисквания към външните запомнящи устройства** – да са надеждни; да са икономични; енергонезависими; високоскоростни; да се използват многократно и т. н.

# Основни характеристики:

⁂ **Време за достъп** – времето за което се намира търсената информация.

⁂ **Капацитет на дисковото устройство** – определя се от произведението на:

броят на повърхностите **x** броят на пътеките на всяка страна **x** броят сектори на пътека **x**

байтовете на всеки сектор.

* **Видове запомнящи устройства** – могат да се класифицират по различни признаци, но най- съществен остава класификацията според метода на запис/четене (*фиг. 3 в приложение*), а именно:

⁂ **Магнитни** – използват намагнитване за запомнянето на данни. Подразделят на такива с **последователен достъп** – магнитна лента (които вече не се използват) и на такива с **пряк достъп** – HDD.

⁑ **Устройства с пряк достъп** – при тях във всеки един момент можем да прочетем файл с данни, намиращ се на произволно място в диска (много по-бързи от лентите).

⁑ **Устройства с последователен достъп** – четенето на данните се извършва последователно,

относително бързо. Последователното четене на данните води до това, че времето за прочитане от различни части на паметта е различно. Ако системата се обърне за информация и тя не е в първата проверена клетка, търсенето продължава в следващите клетки, докато нужната информация не бъде открита.

⁂ **Оптични** – информацията се прогаря с инфрачервен лазер с голяма дължина на вълната върху полимерна основа, като контрола на лъча става чрез метален слой.

⁂ **Магнито-оптични** – флаш базирани – някои от USB-тата работят под този метод.

⁂ **Електронен принцип** – запазване чрез електрически импулси.

# ПЪРВА ЧАСТ

**ЗАПОМНЯЩИ УСТРОЙСТВА В СЪРВЪРНИ КОНФИГУРАЦИИ**

# Флопи диск/FDD

* + 1. **Флопи диск/FDD** – Floppy Disk Drive – е външно запомнящо устройство, използвано до 90-те години на двадесети век (*фиг. 4 в приложение*). Носителят на информацията е гъвкав магнитен диск/дискета. Физическото устройство се състои от записващо/четяща глава, задвижващ двигател, стъпков двигател, управляваща логика, шпинделен двигател, позиционер, механична рамка и електронна платка. Капацитетът е изключително малък в сравнение с новите технологии като SD карти, флаш памети и дискове. Повечето дискети поддържат 1,44 MB данни. В сравнение, малък USB диск с капацитет 8 GB побира 8 192 MB, което е повече от 5 600 пъти повече от капацитета на дискета. 5,25-инчовите дискове са били наречени "флопи", защото опаковката на дискетите е представлявала много гъвкав пластмасов плик/flexible plastic envelope. Флопи диска вече е напълно остарял, но въпреки това има вероятност да се използва в сървърните конфигурации, при архивирането на данни.

# Твърд диск/HDD

* + 1. **Твърд диск/Hard disk drive** – това е дълготраен енергонезависим носител на информация, след инсталирането му в системния блок, представлява постоянната памет на компютъра.

(*фиг. 5 в приложение*)

# Твърд диск – конструктивни особености и физическа организация

Състои се от две основни части – **основен блок** и **електронна схема**.

* **Платка с електроника** – включва централен специализиран процесор, постоянна ROM памет, оперативна RAM за кеш памет на харддиска, сигнален процесор и схеми за връзка с интерфейса.
* **Електронната схема** – включва управляващия софтуер и кеш памет и предусилвателните управляващи сигнали. HDD може да включва 1 или повече дисковидни плочи.
* **Основният блок** – включва всички механични, движещи се части – метални (алуминиеви) дисковидни плочи (магнитните плочи са изработени от алуминий или керамика, стъкло върху които е нанесено хромно покритие), двигатели, магнитни глави и серводвигател.

Повърхността на плочата е покрита с метално-оксидно покритие с феромагнитни свойства. Когато плочите са повече се укрепват около ос, наричана шпиндел и формират така наречения

дисков пакет. Шпинделът държи дисковия пакет и така ги държи да не се приплъзват. За целта формата на шпиндела е на пресечен конус (*фиг. 6 в приложение*).

Всяка плоча е покрита едностранно или двустранно с работна повърхност, при по-старите HDD с медно-оксидно покритие с магнитни свойства, а при по-новите с карбоново покритие. В зависимост от броя на дисковете и работните повърхности се определя и броя на магнитните глави, тоест за всяка работна повърхност трябва да има отделна глава за запис/четене на информацията. Когато магнитните глави са повече, се укрепват върху рамо със специфична форма, което трябва да осигурява радиално придвижване на магнитните глави над работните повърхности от периферията към центъра на дисковидните плочи. Рамото се задвижва от електродвигател. Физическата организация на HDD се свързва с конструктивните особености – става въпрос за работни повърхности, писти и сектори.

* **Работната повърхност** се разделя на малки сектори с капацитет по 512 байта. Тези 512 байта са стандартни за всички дискове, но операционната среда може да промени размера от 512 до 4096 байта. 7-8 сектора правят 1 **клъстер** (клъстер – съвкупност от няколко сектора). В тези байтове се съдържа адрес на сектора, информация за дефектност и място за записване на информацията. HDD e херметически затворен и това се прави с цел да се предпази от навлизане на фини прахови частици, които могат да попаднат между диска и главата. Магнитната глава не трябва да опира работната повърхност на плочата, за да не се получават повредени сектори (краш/bad сектори). Магнитната глава се държи на отстояние от работната повърхност около 0,15 нанометра, чрез така наречените въздушни възглавници. През отворите на магнитната глава се пропуска въздух с високо налягане, който ще се движи с висока скорост от магнитната глава към повърхността на диска.
* **Цилиндъра** е мислена повърхност, която се образува от позиционирането на няколко магнитни глави, върху една и съща писта от различни повърхности. Съхраняването на данни върху магнитни носители се базира на цифровия магнитен запис. За целта трябва да има взаимодействие между диска и магнитната глава. Всяка от магнитните глави се състои от магнитопровод с процепи и четящо-записваща намотка от проводници. В режим запис, на намотката се подават токови импулси с различна полярност (–; +), в зависимост от това какво трябва да се запише (0, 1). Създават се магнитни полета, чиито силови линии са с обратен поляритет на токовите импулси. Тези силови линии се „прехвърлят“ през процепите на магнитните глави и където попаднат върху работната повърхност намагнитват много малък участък (точка) с логически еквивалент 0 или 1-ца. Тези малки участъци се наричат още домени. Рамото позволява радиално обхождане на плочите от периферията към центъра и обратно.

Когато две глави се опитват да се позиционират върху една и съща писта от различни повърхности, формират мисловна повърхност, наречена цилиндър (*фиг. 7 в приложение*).

При внезапно спиране на захранването, при изпускане на HDD може да се получи така нареченото „**паркиране**“ на магнитните глави, тоест прибират се към шпиндела. За това около центъра на дисковидните плочи има работно покритие, но липсват записи. При изпускане на PC или HDD, освен паркиране може да се получи и така нареченото „заключване“.

# Основни характеристики на HDD

⁂ **Капацитет** – количество информация, което може да се запише (от MB, GB, TB).

**Формула**: *капацитет на HDD = брой цилиндри* ***x*** *брой глави* ***x*** *брой сектори* ***x*** *512B (размер на сектора).*

⁂ **Скорост на обмен/Data transfer rate** – MB/s – зависи скоростта на въртене на самия диск, размера на блока, кеша, скоростта на въртене (обороти: 4 200, 5 400, 7 200, 15 000) и т.н.

⁂ **Скорост на въртене** – 4200 оборота/мин – за ноутбуци; 5400-7200 – за персонални компютри;

от 10 000 до 15 000 оборота – за сървърни конфигурации.

⁂ **Производителност** – зависи от времето за позициониране и скоростта на трансфер/предаване на данните. Времето за позициониране има 2 части – seek time; latency.

⁑ **Seek time** – времето, необходимо на главите да се преместят от една позиция в друга – измерва се в милисекунди. Големината му зависи от разстоянието между двете позиции. Винаги се изчислява средно – 4-10 милисекунди.

⁑ **Latency** – синхрона между въртенето на плочите и преместването на главите, именно изчакването на главата, така че въртенето на плочите да докара дадената пътечка за четене. То зависи от скоростта на въртене. Измерва се в милисекунди. Двете времена служат за сравняване на два диска.

⁂ **Вътрешна скорост за обмен** – зависи много от типа интерфейс.

# ⁂ Средно време за безотказна работа

⁂ **Размер на плочите** – 3,5′′; 5,25′′

# ⁂ Ниво на шум

⁂ **Физически обем на хард диска**

⁂ **Дисков интерфейс** – начина по който се предават данните, след като се прочетат от плочите – IDE/ EIDE (ATA) SATA.

* + 1. **Логическа организация на HDD** – свързва се с избор и инсталиране на операционната система, която дава възможност HDD да се разделя на отделни дялове (партишъни), които операционната среда вижда като отделни устройства. При логическа организация, всичко което се записва върху хард диска е файл. Най-високо в логическата йерархия е логическият дял. Той се формира от N-та брой последователни цилиндъра. Хард дискът може да се разделя на множество дялове. Файловете се записват на части – блокове – клъстери. Всеки блок/клъстър съдържа N брой последователни сектора.
* **Предимствата от разделянето на HDD на отделни дялове** са:

1. По-бърза работа с диска при фрагментиран дял.
2. Възможност за използване на няколко операционни системи на един компютър.
3. По-лесно възстановяване на информация след атаки на злонамерен софтуер.

* Операционната среда комуникира с хард диска чрез използване на **файлови системи** – FAT/ FAT 32, NTFS и други. Файловата система FAT 32 се смята за бързо оборотна система за малки дялове, използвана при по-старите харддискове. При по-новите дискове заради по-големия им капацитет се използва файлова система NTFS.

Когато се записва нов файл, винаги се започва от празен цилиндър, до запълване на цялото пространство и ако файла е прекалено голям, то фирменият софтуер търси друго свободно пространство. Блоковете от всеки файл се записват в последователни цилиндри и дори да има свободно пространство от текущия цилиндър, записа на следващия файл ще започне от нов цилиндър. Един дял е фрагментиран, когато блоковете от данни не са разпределени на последователни цилиндри. С фрагментирани дялове се работи трудно – необходимо е време за намиране на съответния сектор и за придвижване на главата до него. Диска се дефрагментира чрез специален софтуер. Всеки блок от файла има номер за инициализация и тъй като файловете са много, се получава особена структура данни, която се съхранява на фиксираното място в този дял. Тази структура се съхранява в папка-файл, в която се намира и самия файл с неговите атрибути – име, големина, дата, час разширение, версия и т.н.

При повечето файлови системи информацията се дублира – NTFS, NTFS1, NTFS 2. При NTFS файлова система има възможност да се направи по-голямо уплътняване на записите по периферията на диска, отколкото към центъра, получава се така наречения зонален запис при работа с големи файлове.

Файловата система определя начина на организиране и съхраняване на данните върху носителите на информация, дефинира се формата на физическото съхранение на информация

като от нея зависи размера на името на файла, неговия максимален размер и инструментите които могат да се използват.

* + - 1. **NTFS файлова система** – New technology file system – е по-стабилна. Заменя файловата система FAT и става предпочината файлова система в операционна система Microsoft Windows. NTFS е значително подобрена спрямо FAT и HPFS (high performance file system). Подобренията включват поддръжка на метаданни и използване на по-сложни структури от данни за подобрение на производителността, сигурността и управление на мястото на диска. Добавени са допълнения като списъци за контрол на достъпа и водене на дневник на файловата система.
* **Предимствата от използването на NTFS** – NTFS е по-бърза при работа с големи файлове и колкото е по-голям файла, толкова е по-ефикасна; NTFS се фрагментира по-трудно и по-рядко; NTFS оползотворява пространството по-добре; NTFS е по-стабилна и по-издръжлива; NTFS е по-сигурен; Могат да се поддържат файлове над 4 GB; изпълнява се добре дори в дяловете над 400 MB; структурата на файлове и директории подобрява производителността; NTFS предлага дискови квоти.
* **Недостатъците от използването на NTFS** – ограничения за именуването на файловете; несъвместимост с Windows 95, 98, ME и DOS.
  + - 1. **FAT файлова система** – File Allocation Table – файлова система за флаш устройства, създадена от Microsoft. FAT 16, FAT 32 – числото след FAT показва броя битове, които файловата система използва за да адресира клъстерите.
      2. **ExFAT файлова система** – Extensible File Allocation Table – файлова система за виста, за форматиране на флаш устройства и карти.
      3. **UDF файлова система** – Universal Disk Format – използва се при оптичните носители, използва се за четене и записи. Използва се от Windows 95.
* **Предимствата от използването на UDF** – сравнително ниска цена; енергонезависима; сравнително голям обем; малко време за достъп; лесно администриране.

# Солид стейт драйв/SSD

* + 1. **Същност на SSD/Solid state drive** – полупроводниково дисково устройство или статично дисково устройство. Енергонезависима компютърна памет, основаваща се на флаш паметите (*фиг. 8 в приложение*). За разлика от хард диска, SSD не съдържа никакви механични части. Като полупроводников елемент се използва силиций и в зависимост от използваната памет могат да бъдат: SRAM; DRAM; Flash-nand памет устройства. SSD дисковете използват енергонезависима Nand flash памет и са с възможност да съхраняват данните без постоянно

захранване. Тези устройства, които работят с flash памет са по-бързи, но и по-скъпи. Flash паметта има ограничение на броя пренаписвания. Смята се, че SSD предлага най-бързият енергоефективен начин за съхранение и споделяне на информация. Предлагат много по-бързи скорости за четене и запис. SSD устройството е вградено в компютъра и да работи с помощта на микросхеми. При HDD, четенето и писането става с намагнитване и размагнитване на малки части, докато при SSD става с активиране и деактивиране на клетки, чрез внезапни спирания на захранването.

# Видове памет и ресурс на SSD дисковете

* **Клетка с 1 ниво** – **SLC/Single Level Cell** – основава се на 1 клетка, която се активира- деактивира. Този тип е доста издръжлив и позволява многократно презаписване. Предимствата: многократно презаписване = 100 000 пъти; скоростта на четене; надеждност и издръжливост на високи температури. Недостатък е, че са много скъпи.
* **С многостепенни клетки** – **MLC/Multi Level Cell** – поддържат от 3 000-5 000 презаписвания, висока издръжливост, достъпна цена. Значително по-надеждна от TLC, но не са по-надеждни от SLC.
* **С тристепенна клетка** – **TLC/Triple Level Cell** – от 3 000-5 000 презаписвания. Най-слабите от тази сфера, но въпреки всичко са 10 пъти по-бързи от HDD. Доста по-бавни от SLC и MLC, износват се бързо и се използват при по-стари машини.
* **V**-**3D NAND** – свръхбърза тип памет (с най-известен производител Samsung) – многократни възможности за презаписване. При този тип клетките се подреждат вертикално, а не хоризонтално. Най-голямото предимство е огромното количество памет (първият такъв диск е бил 4 терабайта).

# Опции за съхраняване на данни на SSD устройство

⁂ За ускоряване на Windows, за по-бърза работа с офис пакет – 60-64 GB.

⁂ При работа с видео и графични редактори 120-128 GB.

⁂ При геймърски конфигурации 240-256 GB.

⁂ Производители – Intel, Sand force, Marvel, Adata, Kingston, Samsung.

*Препоръчително е да се използва SSD устройство за ускорение на операционната среда и работа с приложни програми, но не и за архивиране на данни.*

* + 1. **Начини за свързване на SSD** – Sata connector – Sata 3.1; PCI express – по-висока скорост, заради директната връзка с дънната платка; външно SSD – USB; видове контролери – SSD дисковия контролер отговаря за ясната и прецизна работа на всяка клетка. Той определя колко качествен е SSD диска. Може да възникне нечист кеш и това води до падане скоростта.

Скоростта на SSD зависи изключително от скоростта на запис/четене. Повечето SSD четат по- бързо, отколкото записват. Ако кеша е пълен, може да се намали скоростта. Най-бавните SSD са от 3 до 10 пъти по-бързи от HDD.

* + 1. **Размери на SSD дисковете** – миниатюризацията е основна насока; за PC – с диагонал 3,5 инча; за лаптопи 2,5-1,8 инча; за SSD най-популярните форм-фактори са – mSATA, M2 – това са карти за Sata и PCI express шини. Ширината на SSD е 12 мм, а дължината от 16 до 11 мм. Дефрагментацията при SSD не е препоръчителна (забранена).
    2. **Съпоставителна таблица на Харддиск и SSD –** (*таблица 1 в приложение)*

# Оптични дискови устройства

* + 1. **Компакт диск/Compact disc** – оптичен носител на информация във вид на диск с отвор в центъра (*фиг. 9 в приложение*). Информацията се записва и чете с помощта на лазер. При CD и DVD дисковете се използва червен лазер, който работи в инфрачервената област. Самият компактдиск се изработва от поликарбонат с дебелина 1.2 мм и е покрит с много тънък слой алуминий. Върху алуминия се поставя защитно покритие от лак и върху него се отпечатва етикета. Информацията върху диска се записва във вид на спирална пътечка, чрез така наречените питове/pits, издълбани в поликарбонатния слой. Материалът от кoйто е изготвен запомнящият слой, зависи от типа на оптичния диск – органична боя или специална сплав (*фиг. 10 в приложение*).
    2. **Видове компакт дискове** – **CD-ROM** – за производствен запис; **CD-R**, **CD-WORM** – за еднократен запис; **CD-RW** – за многократен запис.
* **CD-ROM** – Read Only Memory – само за четене, с формата на аудио компакт-дисковете; многофункционални – в един участък само за четене, а в друг и за запис. Записът се реализира по време на производството на диска. Имат еднакъв формат и капацитет от 650 MB. Диск с диаметър 120 мм, дебелина 1,2 мм и централен отвор с диаметър 15 мм. Слоят на подложката на записващия CD-ROM (CD-R) е покрит с органичен слой за запис, слой злато и слой лак.
* **CD-R** – Read – вид компакт диск, който позволява еднократен запис на музика или данни в произволен логически формат. Дисковете за еднократен запис се различават от необикновените компакт дискове, по това че имат допълнителен слой, нанесен между пластмасовата подложка и металният отразяващ слой. При запис, вследствие от загряването на допълнителният слой, с помощта на лазерно лъчене, се извършват необратими химически промени в диска. Ще се променят както геометричният размер на загрятото петно, така и отразителната способност на

диска в съответната точка. Образува се пит/pit. Записът се реализира от притежателя на диска. При CD-R е еднократно. Запомнящият слой е във вид на органична боя.

* **WORM** – Write Once Read Many – с еднократен запис – поради необратимост на процесите, съпътстващи записа. За разлика от обикновените CD-та, отразителният слой не е от алуминий, а от сребро, понякога и от злато.
* **CD-RW** – Read Write – презаписваеми, с многократен запис. Записът се реализира от притежателя на диска. При CD-RW, презаписването е многократно – до 1 000 пъти. Запомнящият слой при CD-RW е специална сплав.
  + 1. **DVD устройства** – Digital Video Disk – с капацитет от 4,7 до 18,8 GB. DVD дисковете са алтернатива на видео касетите, при които записът е бил аналогов. Технологията на DVD е усъвършенствана от тази на CD технологията, като всяка една от подложките на DVD диска, може да носи един или и два информационни слоя, което позволява да се постига по-голям капацитет.
* **Видове DVD дискове** – DVD-R; DVD-R+; DVD-RW и DVD-RAM.

Основен недостатък е, че капацитетът им не е достатъчен за 4К и 8К качество с продължителност на филм.

# Стандарти – DVD 5, 9, 10, 14, 18

⁂ **DVD 5** – 4.7 GB едностранен еднослоен стандарт.

⁂ **DVD 9** – 8.5 GB едностранен стандарт при еднослоен или двуслоен.

⁂ **DVD 10** – 9.4 GB едностранни и двуслойни.

⁂ **DVD 14** – 12.3 GB двустранен диск с една двуслойна страна и една еднослойна страна.

⁂ **DVD 18** – 17.1 GB двустранен и двуслоен.

* + 1. **Blu-Ray дискове** – алтернатива на DVD като предлагат цифрови записи с високо качество. Записът се постига с висока плътност и лазерен лъч, който е в синия или виолетовия спектър. В този спектър, лъча може да се фокусира върху по-малка площ и по този начин може да се запише повече информация на един носител. Blu-ray дисковете са оптични дискове с висока плътност на записа. Предназначени са за съхранение на цифрови данни, включително видео с висока разделителна способност – high definition video. Името Blu произлиза от използваното синьо лазерно излъчване, което позволява запис/четене на данни върху оптичен носител.
* Според физическия им формат се делят на:

⁂ **Еднослойни** – 25 GB.

⁂ **Двуслойни** – 50 GB.

⁂ **Трислойни** – 100 GB.

⁂ **Четирислойни** – 128 GB възможност за запис.

* + 1. **HVD дискове** – Holographic Versatile Disc – холограмни дискове. Записът се извършва чрез кодиране. Използва се за архивиране на данни от компаниите. До 400 GB капацитет.
    2. **Параметри и характеристики на компакт дисковете** – информационен капацитет на диска; размери, съответствие със стандартите; интерфейс – (SCSI-2, MAC и PC-AT); internal, external; формати; средно време за достъп до информацията; скорост на обмен; честота на поява на грешки след корекцията; Constant Linear Velocity.
    3. **Предимства на оптичните запомнящи устройства** – ниска цена; могат да се презаписват над 100 000 пъти; трайно съхранение на информацията, десетки години наред; възможност за съхраняване върху едни и същ тип носител на различни типове и форми информация – аудио и видео, цифрова и аналогова; липса на износване и т.н.
    4. **Недостатъци на оптичните запомнящи устройства** – необратимост на процеса на запис при повечето оптични дискове; най-малки дефекти могат да доведат до загуби на съществени обеми информация; сравнително бавен запис; липсата на стандартизация, както в размерите на носителите, така и във форматите на данните, интерфейсите, драйверите, свързания с ползването им софтуер.

# ВТОРА ЧАСТ

**СЪРВЪРИ – СЪЩНОСТ, ХАРАКТЕРИСТИКИ И КЛАСИФИКАЦИЯ. RAID МАСИВИ.**

# Сървър/Server

* 1. **Сървър определение** – обслужващо мрежите устройство. Зад всяка функция на мрежа или предлагана мрежова услуга, стои сървър. Сървърът е компютър, който работи съвместно с други компютри, като се различава по това, че за работата му не е необходимо човешко участие (*фиг. 11 в приложение*). Предназначен е да обработва заявки, да предоставя данни и услуги към останалите компютри/клиенти, по интернет или в локална мрежа. Той е или софтуерно, или хардуерно устройство. Наименованието идва от архитектурата клиент-сървър.

Някои сървъри са ангажирани с конкретна задача – **специализирани**, но повечето съвременни сървъри са **споделени** – поемат отговорността (за електронна поща, DNS, FTP и за множество уебсайтове в случай на уеб сървър).

Разпределението на дейностите в мрежата, облекчава работата й и я прави по-ефективна.

# Компоненти на сървъра

* **Хардуерни компоненти** – изискванията към хардуера зависят от предназначението на сървъра и софтуерa му. Обикновено се състоят от: системна платка/motherboard, един или повече процесори, RAM, памет за съхранение (обикновено харддиск, в някои случаи SSD), мрежов интерфейс, шаси за монтиране в шкаф и захранване/power supply (*фиг. 12 в приложение*). Повечето сървърни хардуерни устройства поддържат извънлентово управление чрез специален мрежов порт. То позволява управление и наблюдение на сървъра. Системите за извънлентово управление могат да се използват за дистанционно включване или изключване на сървъра, за инсталиране на операционна система и наблюдение на състоянието. Тъй като достъпът до сървърите масово се осъществява по мрежа, голяма част от тях работят без надзор, без монитор или входно устройство, аудиоапаратура и USB интерфейси. Много нямат графичен потребителски интерфейс (GUI). Дистанционното управление може да се извършва чрез различни методи, като някои от тях са: Microsoft Management Console (MMC), PowerShell и т.н.
* **Софтуер** – сървърът се нуждае най-малко от два софтуерни компонента – **операционна система** и **приложения**. Операционната система действа като платформа за изпълнение на сървърното приложение. Тя осигурява достъп до основните хардуерни ресурси и дава възможност за мрежова свързаност. Също така осигурява средствата за комуникация на клиентите със сървърното приложение. Преобладаващите операционни системи сред сървърите са подобни на UNIX

дистрибуции с отворен код, като – базирани на Linux и FreeBSD. Windows Server също имат значителен дял. Собствени операционни системи като z/OS и macOS Server също се използват, но са с по-малък дял. Специализираните сървърно ориентирани операционни системи обикновено имат характеристики като: графичен потребителски интерфейс, който не е задължителен; възможност за преконфигуриране и актуализиране на хардуера и софтуера до известна степен без рестартиране; усъвършенствани средства за архивиране, позволяващи редовно и често онлайн архивиране на критични данни; прехвърляне на данни между различни томове/volumes или устройства; гъвкави и усъвършенствани възможности за работа в мрежа; възможности за автоматизация и др.; строга сигурност на системата с усъвършенствана защита на потребителите, ресурсите, данните и паметта; усъвършенствано откриване и предупреждаване за състояния като прегряване, отказ на процесора и диска. Днес много настолни и сървърни операционни системи споделят сходни бази данни, различаващи се най-вече по конфигурацията.

* 1. **Архитектура на сървъра** – (*приложение 1)*

# Изисквания към сървъра:

* **Средства улесняващи инсталирането** – софтуерни пакети, които предпазват от допускане на големи грешки при инсталиране и експлоатация на сървъра и оказват ценна помощ на мрежовия администратор.
* **Средства за наблюдение и контрол** – продукти за визуализиране състоянието на сървъра. Те позволяват автоматизиране на отделни задачи, които претоварените системни администратори пренебрегват.
* **Запаметяване и защита на информацията** – прилагат се различни техники за дублиране на информацията, без това да се отразява чувствително върху крайната цена на сървъра. Използват се три метода:

⁂ **Огледален диск** – два диска използват един и същи контролер, като и двата записват напълно идентично копие на данните. Недостатък – при повреда на контролера информацията се губи.

⁂ **Дублиране на дискове** – всеки от дублиращите дискове разполага със собствен контролер. Методът е по-скъп, но по надежден и осигурява по-голямо бързодействие.

⁂ **RAID** – обобщено наименование на няколко метода за повишаване на надеждността. Данните се записват на няколко диска по определена схема.

* **Средства за отдалечен контрол/Remote access** – много полезни, когато мрежовият

администратор не е наблизо. Той може да се свърже по телефона и да получи информация за състоянието на мрежата, да тества или рестартира системата. Има и възможност, където при възникване на проблем, сървърът автоматично да потърси помощ по телефона.

* **Допълнителни осигуровки на сървъра** – хардуер, който сам фиксира възникналите проблеми в сървъра; **оперативна памет** с автоматична корекция на грешките. Ако това не може да стане, повреденият чип се изолира и се сигнализира за събитието. Двойна осигуровка на **захранването** на сървъра. Включване на два UPS, като допълнителна осигуровка на захранването. Двете устройства работят в паралел; дублиране на сървъра (клъстериране) – две или повече машини се свързват чрез високоскоростна връзка и се прави абсолютно огледален образ на данните и паметта.
  1. **Видове сървъри според тяхното предназначение** – *(приложение 2)*
  2. **Физически и виртуални сървъри** – на база тяхната реализация, се различават физически и виртуални сървъри.
* **Физически сървър** – повечето сървъри са от този тип. Всеки физически сървър включва сървър с дънна платка, памет, процесор, мрежова връзка, твърд диск и операционна система за изпълнение на програми и приложения. Счита се за "bare-metal"/“чист сървър“, тъй като хардуерът му се използва директно от операционна система вместо от платформа за виртуализация.
* **Виртуален сървър** – виртуално представяне на физически сървър. Подобно на физическия, виртуалният включва собствена операционна система и приложения. Те са отделени от всички други виртуални сървъри, които могат да работят на физическия сървър. Процесът на създаване на виртуални машини включва инсталиране на олекотен софтуерен компонент – хипервайзор, на физическия сървър. Задачата му е да позволи на физическия сървър да функционира като хост за виртуализация. Хостът за виртуализация предоставя хардуерните ресурси на физическия сървър – като процесорно време, памет, място за съхранение и мрежова честотна лента – на разположение на една или повече виртуални машини.
  1. **Типове сървъри според големината/натоварването им** – сървърите могат да бъдат разделени и според големината и натоварването, на което са подложени:
* **Бизнес/Корпоративни сървъри** – големите сървъри работят за дълги периоди, без прекъсване. Функционалността на този тип сървъри трябва да бъде непрекъсната, което прави надеждността и издръжливостта на хардуера ключови. Критично важните корпоративни сървъри трябва да са много устойчиви на грешки, да използват специализиран хардуер с ниска честота на повреди, за да се увеличи времето на работа. В системите се включат непрекъсваеми източници на захранване, за да се предпазят от прекъсване на електрозахранването. Сървърите обикновено включват хардуерно резервиране, като двойни захранвания, RAID дискови системи и ECC памет, както и обширно тестване и проверка на паметта преди стартиране на системата. Критичните компоненти могат да бъдат подменяни в горещо състояние/hot swapping, а за да се предпазят от прегряване, сървърите могат да имат по-мощни вентилатори или да използват водно охлаждане. Често срещано е да бъдат

конфигурирани, включвани, изключвани или рестартирани от разстояние, като се използва извънлентово управление. Корпусите на сървърите обикновено са плоски и широки и са предназначени за монтаж в 19-инчови шкафове или в отворени шкафове. Тези типове сървъри се намират в специализирани центрове за данни. Шумът е малък проблем, но консумацията на енергия и отделянето на топлина могат да имат негативно влияние. За тази цел, сървърните помещения са оборудвани с климатични устройства.

* **Малки бизнес и домашни сървъри** – всеки компютър може да действа като сървър с подходящия софтуер. Може да се изтегли програма за FTP сървър на настолен компютър, за споделяне на файлове между потребители в направената мрежа. Някои твърди дискове, работещи в мрежа, използват протокола на сървъра Network Attached Storage, за да позволят на различни компютри в домашната мрежа да имат достъп до споделен набор от файлове. Софтуерът на медийния сървър Plex, позволява на потребителите да гледат цифрови медии на телевизори и устройства за развлечение, независимо дали данните се намират в облака или на локален компютър. За да работи компютър като сървър, той трябва постоянно да работи. Има риск за атаки при свързаност в интернет. Ако има голямо натоварване, компютърът може да не разполага с необходимите ресурси да извърши всички заявки.
* **Мобилни** – за разлика от големите центрове за данни или сървъри в шкафове, мобилният сървър е предназначен за работа на пътя, като в спешни случаи, при бедствия или във временна среда, където традиционните сървъри са неприложими, поради изискванията им за захранване, размера и времето за пускане. Основните ползватели на технологията "сървър в движение" са мрежовите мениджъри, разработчиците на софтуер или бази данни, центровете за обучение, военните, правоприлагащите органи, криминалистите, групите за спешна помощ и организациите за услуги. За да се улесни преносимостта, в шасито са интегрирани функции като клавиатура, дисплей, батерия (непрекъсваемо захранване, за да се осигури резервиране на захранването в случай на повреда) и мишка.
  1. **Работен режим на сървърите** – обикновено се използват за предоставяне на услуги, които са постоянно необходими и за това повечето никога не се изключват. Колкото по-голям е сървъра, толкова е по-важно работата му да не спира, тъй като повече хора разчитат/зависят на него. Когато се повредят могат да причинят проблеми на потребителите и компанията. За това се настройват, така че да са устойчиви на грешки. Тъй като времето за работа е критично важно за повечето сървъри, те работят непрекъснато.

Понякога се изключват умишлено за планирана поддръжка, като в подобни ситуации, някои уеб сайтове и услуги уведомяват потребителите предварително. Сървърите могат да се изключат и

непреднамерено по време на нещо като DDoS атака. Когато даден уеб сървър свали информация за постоянно или временно, е възможно все още да има достъп до нея, ако услуга на трета страна ги архивира. Wayback Machine е пример за уеб архиватор, който съхранява снимки на уеб страници и файлове, съхранявани на уеб сървъри.

Големите предприятия, които разполагат с множество сървъри, обикновено нямат локален достъп до тях с клавиатура и мишка, а чрез отдалечен достъп. Понякога тези сървъри са и виртуални машини, което означава, че на едно устройство за съхранение могат да бъдат разположени няколко сървъра. По този начин се спестява физическо пространство и пари.

* 1. **Начини на свързване на устройствата към сървъра** – при локална мрежа, сървърът се свързва с маршрутизатор, който се използва от всички останали компютри в мрежата. След като се свържат към мрежата, другите компютри имат достъп до този сървър и неговите функции. При уеб сървър, потребител може да се свърже със сървъра, за да разглежда уебсайт, да търси и да комуникира с други потребители в мрежата. Интернет сървърът работи по същия начин като сървъра на локалната мрежа, но в по-голям мащаб. На сървъра се присвоява статичен IP адрес от InterNIC или от уеб хоста. Обикновено потребителите се свързват със сървъра, като използват името на домейна. Когато потребителите се свързват с името на домейна (например "starwars.com"), името автоматично се преобразува в IP адрес на сървъра от DNS резолвера.
  2. **Физическо съхранение на сървърите** – в бизнес или корпоративна среда сървърът и другото мрежово оборудване се съхраняват в шкаф/т.н. рак. Тези помещения помагат да се изолират чувствителните компютри и оборудване от хора, които не трябва да имат достъп до тях. Сървърите, които са отдалечени или не се хостват на място, се намират в център за данни. При тези видове сървъри хардуерът се управлява от друга компания и се конфигурира дистанционно от потребителя или от компанията му.

За малките бизнес/домашните сървъри, не е необходимо специално помещение – може да се намира в някоя стаите, където живее или работи даден потребител. Проблемът би бил евентуалният шум.

* 1. **Съображения при избор на подходящ сървър** – при избора, трябва да се прецени важността на функциите, въз основа на случаите на използване. Възможностите за сигурност също са важни и има доста функции за защита, откриване и възстановяване, които трябва да се разгледат. Ако сървърът ще разчита на вътрешна памет, изборът на типове дискове и капацитет е важен, тъй като може да окаже значително влияние върху входа/изхода (I/O) и устойчивостта. Много организации намаляват броя на физическите сървъри в своите центрове за данни, тъй като виртуализацията позволява на по-малко сървъри да се хостват повече работни натоварвания. Навлизането на

облаците е променило броя на сървърите, които организацията трябва да хоства на място. Събирането на повече възможности в по-малко кутии, може да намали общите разходи, площта на центровете за данни и нуждите от енергия и охлаждане. Обаче хостването на повече работни натоварвания в по-малко кутии може да представлява и повишен риск за бизнеса, тъй като повече работни натоварвания ще бъдат засегнати, ако сървърът се повреди или трябва да бъде изключен за рутинна поддръжка. Контролният списък за поддръжка на сървъра трябва да обхваща физическите елементи, както и критичната конфигурация на системата.

* 1. **Изграждане на домашен сървър или такъв за нуждите на малка фирма** – в съвремието почти всички сървърни услуги може да се ползват чрез облак/cloud, или да се ползват сървъри под наем. Но има причини, поради които изграждането на собствен сървър е предпочитано начинание. За много потребители, от най-голямо значение е контролът на данните. Големи корпорации като Google Drive (*фиг. 13 в приложение*) твърдят, че не притежават данните, които потребителите качват в облака, но в действителност притежават лиценз за възпроизвеждане и модифициране на файловете на потребителите. Ползването на собствен сървър гарантира стриктен контрол на потребителя върху собствените му данни.
  2. **Цена** – цената на хардуера е само едно от перата, за които трябва да се планира бюджет. Други важни разходи са – операционна система; сървърен софтуер; поддръжка на хардуера и софтуера; подмяна на захранването и охлаждане в случай на необходимост и т.н.

**Движение на цените –** благодарение на технологичната еволюция има драстичен спад на цените, не само на професионалните сървърни конфигурации, но и на потребителските системи (*фиг. 14, 15 в приложение*). Всичко това прави достъпно изграждането на сървърна конфигурация за лични цели или за нуждите на малка фирма. На българския пазар от финансова гледна точка, за такива цели са още по-достъпни и вносните, втора употреба професионални компютърни конфигурации. От 1999 г. насам, цената на сървър се е понижила четирикратно в сравнение с пика през 1999 г., когато много RISC/Unix и IBM мейнфрейм машини са се продавали страшно добре. От 20 000-30 000 долара в края на ХХ век, днес цените на сървърните конфигурации за бизнес цели са към 5 000 долара. В подобни диапазони е и движението на цените на персоналните компютри.

* 1. **Глобална консумация на енергия, дължаща се на сървъри** – (*приложение 3)*

# Конфигуриране на дискове

Най-разпространената реализация за конфигуриране на множество твърди дискове е чрез RAID масиви, която се предлага в редица стандартни и нестандартни конфигурации. Макар RAID

масивите да са най-ефективния и разпространен начин за управление на множество дискови устройства, не е единствената възможност. Съществуват и други като:

* **JBOD** – Just a Bunch Of Disks/Kупчина дискове – множество твърди дискове, работещи като отделни независими такива. Не предлага никакво подобрение на производителността и няма никаква резервираност, но предимство е, че не се интересува от това, какви дискове влизат в него.
* **SPAN** или **BIG** – метод за комбиниране на свободното пространство на няколко твърди диска от "JBoD" за създаване на обхватен том. Такова обединяване понякога се нарича също BIG/SPAN. SPAN или BIG обикновено е само разтеглен том, тъй като често съдържа несъвместими типове и размери на твърди дискове (*препратка 2, 3 в приложение*).
* **MAID** – Massive Array of Idle Drives/Oгромен масив от неактивни устройства – архитектура използваща стотици до хиляди твърди дискове за осигуряване на близко до линията съхранение на данни, предназначена предимно за приложения от типа "Write Once, Read Occasionally" (WORO), при които увеличената плътност на съхранение и намалената цена се търгуват за увеличена латентност и намалена резервираност.

# RAID масиви

* 1. **Същност на RAID масивите** – Redundant Array of Independent Disks – набор от дискови устройства, които се управляват от специален контролер, като компютъра ги счита за един независим диск с голям капацитет (*фиг. 16 в приложение*). Основната цел е подобряване на производителността и намаляване на риска от загуба на данни при възникване на технически проблеми или унищожаване на хард дисковете. Райд масивите функционират, като разпределят балансирано информацията върху определено количество дискове. Съществуват различни логически схеми за разпределяне на информацията и те са пряко свързани с производителността на райд масива, с дублирането и защитаването на данните, а или и двете едновременно. Различните дискове се свързват към така наречените райд хардуерни контролери.
  2. **Техники за разпределение** – съществуват две техники за организиране данните в нива на HDD. Това са – data mirroring, data striping.
* **Data mirroring/Дублиране** – информацията се записва огледално на 2 диска. При този вид има резервираност на данните при отпадане на единия хард диск. Това означава, че данните ще бъдат изцяло налични при възникване на технически проблем. Недостатъкът е, че ефективно използваното пространство е по-малко. Използват се 2 пъти повече носители и времето за запис е по-бавно, защото трябва да се запише на 2 места едновременно.
* **Data striping/Разпределяне** – данните се разделят на части, които трябва да се запишат – четни на единия диск и нечетни – на другия. По този начин, те са равномерно разпределени из дисковия масив. Това е предпоставка за по-бързото им прочитане. Дисковото пространство се използва по- пълноценно, защото информацията не се копира на няколко диска едновременно, но за сметка на това се губи резервираността на данните.

Разпределянето на данните между самите дискове се извършва на различни нива – **райд нива**.

* 1. **Стандартни/Основни RAID нива са** – RAID 0, RAID 1, RAID 2, RAID 3, RAID 4, RAID 5, RAID 6, RAID 7 – (*приложение 4*)
  2. **Комбинирани/Хибридни RAID нива са** – RAID 0+1, RAID 1+0, RAID 3+0, RAID 5+0, RAID 5+3 и т.н. – (*приложение 5)*
  3. **Типове райд масиви** – един RAID масив може да бъде създаден както чрез отделно хардуерно устройство, така и софтуерно като част от операционната система. Най-често хардуерните RAID устройства се наричат RAID контролери.
* **Хардуерен RAID масив** – изгражда се с помощта на хардуерно устройство, наречено RAID контролер. Те представляват отделен микропроцесор със собствена памет, обединени на една обща платка, която се добавя към разширителите слотове на основния компютър или сървър. Модерните RAID контролери имат вграден кеш за увеличаване на бързодействието. Дисковете, които ще участват в масива се свързват към този RAID контролер. Най-често RAID контролерите са производство на дадена компания и разполагат със собственически затворен код. По-съвременните RAID контролери имат вграден кеш за увеличаване на бързодействието. Съдържанието на този кеш би било загубено при спиране на захранването на контролера. Поради тази причина, съдържанието на кеш паметта често е резервирано от BBU (Backup Battery Unit) или BBN (Battery Backup Module). Те позволяват на RAID контролера да запамети информацията, която все още не е записана на диска. Това устройство може да осигури резервно захранване на контролера, така че той да запази информацията до 72 часа без захранване. След като бъде възстановено основното захранване на системата, BBU частта ще запише съдържанието на кеш паметта на дисковете на масива. Цялото съдържание на буфера на RAID контролера е невъзстановимо, ако той няма BBU. Много RAID контролери биха функционирали оптимално и с най-висока производителност, ако имат инсталирано BBU устройство.

⁂ **Предимства на хардуерния RAID масив** – висока производителност при по-сложни RAID системи и при ползването на битове за четност; не се използват ресурсите на системата (процесор, памет); възможност за замяна на дискове в работещо състояние (disk hot swapping); по-малко време за възстановяване на масива при отпадане на някой от дисковете; лесен за инсталация – не е нужно

инсталиране и конфигуриране на допълнителен софтуер; при наличие на батерия (BBU) изчакващите записи в кеша на контролера няма да бъдат загубени при спиране на захранването.

⁂ **Недостатъци на хардуерния RAID масив** – допълнителни разходи – хардуерните RAID контролери, струват повече отколкото обикновените дискове контролери; алгоритмите и кодът са затворени собственически от компанията произвела контролера; ограничена възможност за замяна и миграция на дисковия масив; липса на гъвкавост (невъзможност за по-големи промени на масива); високият клас контролери могат да бъдат доста скъпи.

* **Софтуерен RAID масив** – един RAID масив също може да бъде изграден с помощта на отворен код, който се вписва към операционната система. Софтуерният RAID използва споделените ресурси на системата – памет и процесор. Той е по-евтиният вариант в сравнение с хардуерния RAID.

⁂ **Предимства на софтуерния RAID масив** – по-евтин в сравнение с хардуерния RAID, част е от операционната система и не се изискват допълнителни средства за хардуер; отворен код – RAID масивът е независим от хардуера на системата; стандартизирана конфигурация за всяка една операционна система; сравнително добра производителност – процесорите стават все по-бързи; за

сравнително не големи натоварвания и задачи, софтуерният RAID е отлично и евтино решение; гъвкав метод – позволява преконфигурирането на RAID масива по множество различни начини.

⁂ **Недостатъци на софтуерния RAID масив** – по-голяма сложност за изграждане в сравнение с хардуерния RAID. При по-сложни RAID системи и по-високи натоварвания отстъпва по производителност спрямо хардуерните контролери; невъзможна замяна на диск в работещо положение; използва част от ресурсите на системата (процесор и памет); няма възможност за BBU,

тоест при спиране на захранването незаписаната информация в кеша се губи; по-бавно възстановяване на масива; по-голяма подготовка при инсталацията на операционната система.

# ТРЕТА ЧАСТ

**ЗАПЛАХИ И МЕТОДИ ЗА ЗАЩИТА НА СЪРВЪРА**

# Заплахи за сигурността на сървъра

**1.1 Кибер заплаха** – представлява всяка възможна злонамерена атака, която има за цел незаконен достъп до данни, нарушаване на цифровите операции или повреждане на информация. Киберзаплахите могат да произхождат от различни участници, включително корпоративни шпиони, хактивисти, терористични групи, враждебни национални държави, престъпни организации, самостоятелни хакери и недоволни служители. Кибератаките могат да използват чувствителните данни на дадено лице или компания, за да откраднат информация или да получат достъп до финансовите им сметки, наред с други потенциално вредни действия, поради което специалистите по киберсигурност са от съществено значение за запазване на личните данни.

# 1.2. Видове заплахи за сигурността във виртуалното пространство

⁂ **Зловреден софтуер/Malware** – софтуер, който работи без знанието и информираното съгласие на потребителите на дадена компютърна система. Включва компютърни вируси, червеи, троянски коне, ботове, софтуер за шпиониране и други. Може да атакува компютъра на потребителя и/или да атакува други компютри, чрез собствената му система.

⁂ **Техническа неизправност** – може да се получи вследствие на софтуерна грешка, отказ на хардуера, природно бедствие, човешка грешка, злоумишлени действия на служител или външно лице. Обикновено водят до спирането на услуги и прекъсват процеси в организацията. Неизправността може да доведе и до загуба на информация.

⁂ **Нелоялен служител** – съзнателно се стреми да навреди на бизнес или работодател. Може да отпечата, запише и изнесе чувствителна информация, до която има достъп. Най-голяма е опасността от нелоялни служители, чиито служебни задължения включват информационна защита и техническо осигуряване на компютърните системи. Те или имат, или лесно могат да получат неоторизиран достъп до цялата информация.

⁂ **Човешка грешка –** несъзнателно действие или бездействие на служител, което вреди на организацията. Може да е в следствие подвеждане, немарливост или незнание. Тези грешки могат да доведат до заразяване с вреден софтуер, да спомогнат действията на нелоялни или външни лица, целящи да навредят на организацията, да предизвика техническа неизправност или да унищожи

информация, да разкрият чувствителна информация, както се даде достъп до нея през интернет или изгуби електронен носител.

⁂ **Външни атаки** – действия на софтуер или трети лица, които целят да навредят на дадена организация. Тези действия могат да доведат до изтичане или унищожаване на информация или до спиране на определени услуги.

⁑ **Aтака с груба сила** – нахлуващият пробва да влезне, като познае паролата, използвайки софтуер, който ще пробва всяка възможна комбинация, докато не я уцели. По принцип, при много опити на въвеждане на парола, системният администратор бива уведомяван, за да може да вземе някакви мерки.

⁑**Човек в средата/Man in the middle** – извършва се, когато хакери се включват в двустранна транзакция. След като прекъснат трафика, те могат да филтрират и да откраднат данни. MITM атаките често се случват, когато посетител използва незащитена обществена Wi-Fi мрежа. Нападателите се вмъкват между посетителя и мрежата, след което използват зловреден софтуер, за да инсталират софтуер и да използват данни по злонамерен начин.

⁑ **Отказът на услугата/DoS** – вид кибератака, която наводнява компютър или мрежа, така че не могат да отговорят на заявките. Разпределената атака DoS (**DDoS**) прави същото нещо, но атаката се извършва от компютърна мрежа. Кибератаките често използват атака с наводняване, за да нарушат процеса на "ръкостискане" и да извършат DoS. Могат да се използват и няколко други техники, а някои кибератаки използват времето, през което мрежата е изключена, за да извършват други атаки.

⁑ **Фишинг/Phishing** – използва се фалшива комуникация, например имейл, за да се подведе получателят да го отвори и да изпълни инструкциите в него, например да предостави номер на кредитна карта. Целта е да се откраднат чувствителни данни, като информация за кредитни карти и данни за вход, или да се инсталира зловреден софтуер на машината на жертвата.

⁑ **Ботнет атака** – нападателите използват ботнети за автоматично стартиране и разпространение на зловреден софтуер. След това използват ботнетите, за да атакуват или заразяват други машини. Ботнетите/зомби системите, се насочват към и претоварват възможностите за обработка на данни на дадена цел. Тъй като всичко това може да се извършва автоматично, без намесата на потребителя,

бот мрежите могат да се разпространяват много бързо и да бъдат смъртоносни за големи мрежи. Ботнетът е вид DDoS, при който милиони системи могат да бъдат заразени със злонамерен софтуер и контролирани от хакер. Ботнетите се намират на различни географски места и са трудни за проследяване.

# Мерки за защита

В съвремието, компютърната сигурност се състои предимно от превантивни мерки. Въпреки че има многобройни вредители в интернет простанството, може да се използват някои методи, с които да се предпази потребителят.

⁂ Редовно **актуализиране/ъпдейтване на софтуера и операционната система** – с всяка нова версия, разработчиците подобряват услугата си.

⁂ **Ограничение на достъпа до файловете/Restricted access** – предотвратяване разкриването на информация на неоторизирани лица или системи.

⁂ **Използване на VPN** – виртуална частна мрежа/virtual private network е криптирана връзка през интернет от устройство към мрежа. Криптираната връзка помага да се гарантира, че поверителните данни се предават безопасно. Тя предотвратява подслушването на трафика от неоторизирани лица и позволява на потребителя да извършва работа от разстояние (*фиг. 17 в приложение*).

⁂ Защита чрез **поставяне на пароли** – по този начин се ограничава достъпът до конфиденциални данни.

⁂ **SSL сертификати** – протокол, който се използва за защитата на връзката, осъществена от потребителите към сайт. SSL сертификатът криптира данните и защитава канала, по който се извършва комуникацията. Така всички данни, които преминават от браузъра на клиента до уебсайта са криптирани и защитени.

⁂ **Удостоверяване с два фактора/Тwo-factor authentication** – метод за намаляване на достъпа до системата или до чувствителна информация (*фиг. 18 в приложение*). Представлява пращане на потвърждение и/или парола/PIN, до устройство, в което вече е логнат съответният акаунт.

Пример може да е 2-step verification-а на Google, където при правилно въвеждане на потребителско

име и парола, се праща питане до логнатите устройства, дали одобряват достъпа до акаунта.

# Защитна стена/Firewall

* 1. **Определение** – специализиран хардуер или софтуер, който проверява мрежовия трафик, преминаващ през него и разрешава или забранява достъпа по определени правила. Филтрират трафика между вътрешната и външната мрежа по отношение на пренасяната информация, чрез зададени ключови думи и следят за спам, компютърни вируси и троянски коне (*фиг. 19 в приложение).*
  2. **Функции на защитната стена** – представлява граничен контролен пункт за желаещите да преминат пакети. Целият трафик се осъществява през този пункт, който има за задача да пропуска

само това, което е безопасно. При настройка на защитата има два основни подхода – пропускат се всички данни и услуги с изключение на изрично забранените или се забраняват всички данни и услуги с изключение на специално разрешените.

Защитната стена има три основни функции – да блокира данните, за които има вероятност да прикриват хакерски атаки; да скрива информация за мрежата, като маскира IP адреса на мрежата с IP адреса на защитната стена; води дневници/logs за информационния поток със записи на определени събития. Има и още много функции като филтриране на съдържанието/content filtering и откриване на пробиви в системата/intrusion detection.

* 1. **Видове защитни стени** – 3 основни вида – **филтриращи маршрутизатори**, **поддържащи връзката пакетни филтри** и **приложни шлюзове**. Повечето защитни стени са нещо средно между тези видове.
* **Филтриращи маршрутизатори/Filtering routers** – разглеждат всеки пакет отделно – не обръщат внимание на пакета като част от установена връзка.
* **Поддържащи връзката пакетни филтри/Stateful packet filters** – разглеждат всеки един пакет като част от вече установената връзка
* **Приложни шлюзове/проксита/Application gateways/Application proxies** – програми, намиращи се между крайния потребител и публичната мрежа – шлюзовете изпълняват методите вместо крайните потребители, защитавайки ги така от външни опасности. Тези приложения имат силни защитни свойства понеже крайните потребители никога не комуникират директно с хостове в Интернет.

# Съвети за използване на защитна стена

⁂ **Възможно най-често актуализиране/ъпдейтване на защитната стена** – това я поддържа актуализирана срещу всички новооткрити уязвимости. Потребителите на лични и домашни защитни стени могат безопасно да актуализират незабавно. При големите организации може да се наложи първо да проверят конфигурацията и съвместимостта в мрежата си.

⁂ **Използване на антивирусна защита** – само защитните стени не са предназначени за спиране на вируси и други инфекции. Вредителите могат да преминат през защитите на firewall-a и ще е необходимо решение за сигурност, което е предназначено да ги деактивира и отстранява.

⁂ **Ограничаване на достъпните портове и хостове с помощта на бял списък** – по подразбиране трябва да се отказва връзка за входящ трафик. Ограничаване на входящите и изходящите връзки до строг бял списък с надеждни IP адреси. Намаляване на привилегиите за достъп на потребителите до

най-необходимото. По-лесно е да се запази сигурността чрез разрешаване на достъпа, когато е необходимо, отколкото да се отменя и да се намаляват щетите след инцидент.

⁂ **Сегментирана мрежа** – страничното движение на злонамерени участници е ясна опасност, която може да бъде забавена чрез вътрешно ограничаване на кръстосаната комуникация.

⁂ **Разполагане с активни мрежови резерви, за да се избегне прекъсване на работата** – резервните копия на данни за мрежовите хостове и други важни системи могат да предотвратят загубата на данни и производителността по време на инцидент.

# Антивирусен софтуер/Antivirus software

* 1. **Антивирусен софтуер** е софтуерно приложение, предназначено да предпазва и отстранява компютърни вируси и други злонамерени програми. Тези програми, могат да бъдат най-различни, но най-разпространените са троянски коне, червеи и вируси. Работата на антивирусния софтуер е да предпазва компютъра, като непрекъснато следи файловете, които се изпълняват и отварят, за възможни заплахи. Всяка антивирусна програма притежава различен алгоритъм на сканиране и реално е почти невъзможно да открие всички съществуващи вируси. Всяка програма е уникална и притежава различни възможности за защита (*фиг. 20 в приложение*).

# Причини за избор на Norton пред други антивирусни програми/системи

Въпреки че Нортън е платена антивирусна програма, а на пазара има доста безплатни или по- евтини варианти, може да се прецени, че е по-добра опция. През големи периоди в годината, предлагат намаления, които правят цената по-постижима за джоба на потребителите, притежателите и менажиращите сървъри. Към момента, цената на стандартния им вариант е 15 евра, което е приблизително 30 лева за първата година на използване. Освен цената, друг много голям плюс на Нортън е, че предлага много функции освен основното му предназначение.

* 1. **Norton антивирусна** – компютърна програма, осигуряваща предотвратяване и премахване на злонамерен софтуер по време на абонамент и използваща подписи и евристика за идентифициране на вируси. Други включени функции са лична защитна стена/firewall, филтриране на спам по имейл и защита от фишинг. Антивирусната е съвместима с Windows 7 и по-новите поколения, Android (6.0 и нагоре, с изключение на устройствата Huawei, Amazon и chromebooks), IOS, MAC и Linux (*препратка 4 в приложение*).

# Norton се разделя на две части – device security и online security.

* **Device Security** включва – сканиране за вируси на 3 нива – **бързо сканиране** – фокусира се върху местата, които са изложени на най-голям риск; **пълно сканиране** – сканира всяка част от хард диска, включително и външните устройства; **персонализирано сканиране** – сканира избрани файлове и папки.

**Norton Insight** – функция, която позволява да сканира вируси в бъдеще; **norton power eraser** – функция, която премахва дълбоко скрити вируси и зловреден софтуер; **защита в реално време** - когато засече вирус, заразеният файл се премества в карантинна зона. Заради Sonar анализа си, тази антивирусна програма засича заплахи от файлове и сайтове; **защитна стена** – „бял списък“ – доверени програми, които не се блокират от защитната стена. Списъка може да бъде персонализиран с избрани програми; **norton cloud backup** – криптирана памет, която архивира важни файлове. Има няколко опции за архивиране – ежеседмично, ежемесечно, ръчно или автоматично. Облака е с капацитет от 10 до 50 GB в зависимост от плана; **родителски контрол** – ограничаване достъп до избрани сайтове в интернет и ограничаване на рекламите, които излизат на децата. Могат да се създадат до 15 различни профила, всеки с различни рестрикции; **функция school time** – блокира вижданото от детето, докато учи или е на училище.

* **Online security** включва –

**Mениджър на паролите** – запомня всички пароли на потребителя, като е нужно да се запомни само една парола, която служи за отваряне на password manager-a; **auto change password** – създава силни пароли или променя стари слаби, като ги запомня в password manager-a; **VPN** – има включен VPN към всеки един от пакетите; **safe web разширение** – сканира уеб сайтове и проверява дали са безопасни за посещаване; **safe search** функцията променя началната страница, като подбира безопасни сайтове за посещение; **dark web monitoring** – претърсва dark web-a и частните форуми в търсене на лична информация и уведомява, ако информация бъде намерена.

# Криптиране/Encryption

* 1. **Определение** – техника, използваща математика за да трансформира информация по начин, който я прави нечетима за всеки друг, освен изпращача и хората, които ще получат „ключ”. Осигурява силна техническа защита срещу много видове заплахи, която може да се получи лесно. В сферата на сървърите, може да се използва, като се криптират деликатните данни, в случай че някой хакер или крадец се опита да ги достъпи. Така вредителят или ще бъде възпрян от достъпа им, или ще му отнеме време до като успее да ги достъпи.
  2. **Принцип на действие** – нормално четимо съобщение се трансформира в неразбираем формат, който може да бъде разбран само от някого с тайно знание:

*Обикновено текстово съобщение + Криптиращ алгоритъм + Ключ = Объркано съобщение;*

*Декодиращ алгоритъм + Ключ + Объркано съобщение = Обикновено текстово съобщение*

(*фиг. 21 в приложение*)

* 1. **Какво представлява криптирането?** – средство за защита на данни, използващо една или

повече математически техники, заедно с парола или "ключ", използван за декриптиране на информацията. Процесът на криптиране преобразува информацията с помощта на алгоритъм, който прави оригиналната информация нечетима. Когато оторизиран потребител трябва да прочете данните, той ги декриптира, като използва ключ. Ключът е поредица от знаци, използвани в алгоритъм за криптиране на промяна на данните, така че да изглеждат случайни. Така шифротекстът ще се превърне в обикновен текст и оторизираният потребител ще има достъп до оригиналната информация. Криптирането е важен начин за отделните лица и компаниите да защитят чувствителна информация от хакерски атаки.

* 1. **Прилагане на криптирането** – повечето некриптирана информация предавана онлайн е достъпна за сървъри, даващи информация. Използвайки криптиране, онлайн комуникациите се предпазват в желязна обвивка – не могат да бъдат прочетени по време на предаване на съобщението и са много устойчиви на подправяне. Модерното криптиране е много трудно за пробиване, тъй като използва сложна математика, за да обърка информацията и да се убеди, че само един човек, притежаващ правилния ключ може да я подреди – в съвремието, 128-битовото криптиране е стандартно, като повечето банки, военни правителства и т.н. използват 256-битово криптиране.

В някои софтуерни пакети са включени улеснения за потребителя, като – пълни настройки за автоматично криптиране, които само трябва да се включат. Например, когато уеб сайт е конфигуриран както трябва, уеб браузърът може да използва SSL криптиране, за да защити поверителността на информацията, която е изпратена или получена от уеб сървър. То е най-често използваното за защита на пароли и финансова информация. Използването на SSL криптирането на браузъра може да бъде така просто, както е достъпа до сайт с https схема вместо http схема (например **https**://[www.dir.bg](http://www.dir.bg/) вместо **http**://dir.bg); браузърът обикновено се грижи за всички детайли зад сцената (*фиг. 22 в приложение).*

* 1. **Методи на криптиране** – съществуват три основни метода:
* **Симетрична криптография** – използва се само един секретен симетричен ключ за криптиране на открития текст и декриптиране на шифрирания текст.

Пример може да се даде с представянето на азбука с числа – "А" е "01", "B" е "02" и т.н. Съобщение като "Hello there" (здравей) ще бъде криптирано като "08051212152008051805" и тази стойност ще бъде предадена по мрежата до получателя. След като го получи, получателят ще го декриптира, като използва същия метод – "08" е "H", "05" е "E" и т.н., за да получи оригиналната стойност на съобщението (фиг. 23). Ако неоторизирани лица получат криптираното съобщение "0805121215", няма да има никаква стойност за тях, освен ако не знаят методиката на криптиране. Посоченият пример е елементарен, но съществуват много сложни варианти за повишаване на

сигурността.

Подходящ е за отделни потребители и затворени системи. В противен случай, ключът трябва да се изпрати на получателя, а това увеличава риска от компрометиране, ако бъде прихванат от трета страна. Въпреки това, може да се предпочете, тъй като е по-бърз от асиметричния вариант.

* **Асиметрична криптография** – криптира и декриптира данните с помощта на два отделни криптографски асиметрични ключа, известни като "публичен" и "частен ключ". Публичният ключ може да се разпространява открито, например адресът на получателя, докато частният е известен само на собственика. Двата ключа са математически свързани – наричат се ключова двойка/key pair. За извършване на операция са необходими и двата. Например данните, криптирани с частния ключ, се декриптират с публичния ключ. Данните, криптирани с публичния ключ, се декриптират с частния ключ. По този начин се постига удостоверяване на автентичността (*фиг. 24 в приложение*). Метода се използва в големи среди, където се обменя информация между различни партньори. Асиметричното криптиране се използва при обмен на ключове, защита на електронна поща, уеб сигурност и други системи за криптиране, които изискват обмен на ключове в публична мрежа. Проблемът с този вид криптиране е, че е стотици до хиляди пъти по-бавен от алгоритъма със симетричен ключ.
* **Hashing** – използва се за ефективна проверка на целостта на данните от транзакции в мрежа или за проверка на верността на копирани или изтеглени данни спрямо оригинала. Типичните функции за хеширане приемат входни данни с променлива дължина, за да върнат изходни данни с фиксирана дължина. Верността може да се провери, като въпросните данни се прекарват през една и съща хешираща функция и се проверява дали са идентични с оригиналните хеширани данни (*фиг. 25 в приложение*). Хеширането работи, тъй като е много трудно да се възстановят оригиналните данни само с помощта на хеширания изход. Хеширането се използва и защото е трудно за изчисление, което прави възможно добиването на блокове за криптовалутите. Освен това цифровите подписи допълват тези различни криптографски процеси, като позволяват на истинските участници да доказват самоличността си пред мрежата.
* Множество вариации на тези методи с желани нива на персонализация могат да се прилагат в различни приложения на криптографията.
  1. **Криптиране на файлове и дискове** – модерните операционни системи позволяват използване на система от акаунти и пароли, за ограничаване на достъпа до информация на компютъра. Пълно дисково криптиране е предвидено да предпазва съхранявана информация срещу този вид излагане на риск – ако компютърът е откраднат или конфискуван, когато е изключен. Пароли на хард диск са настройки, предлагани от много производители. Те могат да бъдат пуснати с BIOS на компютъра.

Хард диск паролите не криптират никаква информация на хард драйва, а само предпазват диска от сътрудничество с компютъра, докато не е въведена паролата. Съществуват многобройни услуги, които ще разрушат паролите. Хард диск паролата е полезна срещу случайни крадци, но е безполезна срещу професионалисти в сферата (*фиг. 26 в приложение*).

* 1. **Софтуер за криптиране на дискове** – има много инструменти за пълно дисково криптиране. Водещи програми за дисково криптиране са BitLocker, FileVault и т.н. Някои от тях идват с операционната система, докато други са добавяни от трета страна. Всяка от тези системи може да предпазва данните по-добре, отколкото ако няма никакво криптиране на диска.

# Бекъп/Backup

* 1. **Бекъп** – процес на копиране на файлове или бази от данни от основно на вторично място, така че да се съхранят, в случай на повреждане на оборудването или при други злополуки (*фиг. 27 в приложение*). Данните са жизнената сила на съвременните организации и загубата им може да причини големи щети и да наруши бизнес операциите. За това бекъпването на данните е от решаващо значение за всички големи и малки предприятия. Наименованието на процеса идва от английски – „to back up”/“да имам резервен план“. Процесът включва копиране на наскоро актуализирани или създадени файлове, заредени на сървъра, като това може да включва документи, мултимедийни файлове, конфигурационни файлове, операционни системи и файлове на регистъра. Казано с няколко думи, това са всички данни, които потребителят желае да запази. Backup-а е рутинна част от операциите на големите корпорации с големи сървърни зали, но и на администрираните от по-малките компании компютри. За потребителите на персонални компютри, бекъп-а е също необходим, но масово е пренебрегван. Възвръщането на файловете от backup се нарича restore. Backup технологиите осигуряват за дълго време възможност за ефективно възстановяване на системите от повреди като – човешки грешки, повреди в хардуера на системата, големи природни бедствия и т.н. За малък период от време възстановяват големи размери изгубена информация и обновяват цялостна система към напълно работен вид. Тенденцията е, че времето което се изисква за направата на резервно копие на данни намалява и способността бързо да се възстанови информация значително се подобрява. Чрез ефективно прилагане на backup, компаниите могат да увеличат производителността и надеждността на тяхната **disaster recovery** (пълно възстановяване системата, в случай на бедствия, изгаряне на хардуер и др.) инфраструктура на разумна цена.

# Видове бекъп, според локацията им на съхранение

* **Локален бекъп/Local backup** – опциите за локален backup са няколко, като в зависимост от

нуждите зависи и цената им. Може да се съхраняват критичните файлове на дискети. Този подход е масово използван от хора, които държат данните си за финанси на персоналните компютри. Много програми, свързани с управление на парите постоянно напомнят на потребителите, когато излизат да съхраняват данните. Ако твърдият диск се развали ще може да се възвърне файла. Подхода е доста остарял, тъй като дискети се използват много рядко, но вместо тях може да се използват флашки или преносими твърди дискове. Друг вариант за бекъп е съхранението на данните от целия твърд диск на външен носител, примерно преносим твърд диск.

* **Интернет бекъп/Internet backup** – друга опция за съхранение на важна информация е като се изпрати на друго място за съхранение. Така в случай, че диска се развали, информацията може да се изтегли.
  1. **Видове бекъп, според реализацията им** – има много на брой видове бекъп и условия, когато става въпрос за съхраняване на дигитална информация (*фиг. 28 в приложение*).
* **Цялостен бекъп/Full Backup** – всички файлове и папки избрани за съхранение ще бъдат бекъпнати. Когато последващ бекъп е пуснат, целия списък от файлове ще бъде бекъпнат отново.

⁂ **Предимства** – възстановяването на файлове е бързо и лесно за управление, имайки предвид, че целия списък със файлове и папки е във един бекъп файл; лесно за поддържане и възстановяване от различни версии/дати.

⁂ **Недостатъци** – бекъпа може да отнеме много време, защото всички файлове и папки се съхраняват всеки път, когато той се стартира; използва много дисково пространство, в сравнение със другите типове бекъп (incremental и differential); едни и същи файлове се съхраняват всеки път, като резултата от това е недостиг във дисковото място.

* **Нарастващ бекъп/Incremental Backup** – съхранява всички промени, които са извършени от както е бил извършен последния full или incremental бекъп. При него един full бекъп е стартиран в началото и последващите бекъпи стартират само съхранявайки само промените направени от последния бекъп. Резултата от това е много по-бърз бекъп и по-малко дисково пространство, заето от него.

⁂ **Предимства** – много по-бързи бекъпи; ефективно използване на дисковото пространство – много по-малко заето място, в сравнение с цялостния бекъп и с differential бекъпа.

⁂ **Недостатъци** – restore операциите са по-бавни в сравнение с full и differential бекъпите; restore

операциите са също и по-сложни, тъй като е нужен целият набор от бекъпи, а именно първият full бекъп и всички последващи incremental бекъпи, за да се извърши възстановяването.

* **Differential backup** – съхранява всички промени направени от последния full бекъп. При него един цялостен бекъп се прави в началото и последващите бекъпи се стартират, съхранявайки

промените направени от последния full бекъп.

⁂ **Предимства** – много по-бързи бекъпи в сравнение с цялостния; по-ефективно използване на дисковото пространство отделено за бекъп в сравнение със цялостния, тъй като само променените файлове от последния цялостен бекъп се копират с всеки стартиран differential; по-бързо възстановяване на файловете в сравнение със incremental вида.

⁂ **Недостатъци** – изискват повече време в сравнение с Incremental бекъпа; използването на дисковото пространство не е толкова ефективно, колкото при incremental бекъпа. Всички файлове добавени или редактирани след като е бил стартиран последния цялостен бекъп ще се дублират отново с всеки последващ стартиран differential бекъп; възстановяването на файловете е по-бавно

отколкото при цялостния бекъп; restore операциите са малко по-сложни отколкото при full бекъпа, но са по-лесни отколкото при incremental. Набор от цялостния бекъп и нужния differential бекъп е нужен за да се изпълни възстановяването.

* **Огледален бекъп/Mirror Backup** – „отражение“ на източника се съхранява. С огледалния бекъп, когато файл при източника бива изтрит, то този файл в скоро време се изтрива и от огледалното копие. Точно поради тази причина, mirror бекъпа трябва да се използва с предпазливост, като се има предвид, че ако се изтрие един файл по невнимание или от вирус, то се изтрива и от mirror бекъпа.

⁂ **Предимства** – бекъпа е чист и не съдържа стари или вече ненужни файлове.

⁂ **Недостатъци** – има вероятност файла на източника да се изтрие по невнимание, чрез саботаж или чрез вирус, като той също ще бъде изтрит и от mirror бекъпа.

* **Облачен бекъп/Cloud Backup (Online and Remote backups)** – този вид бекъп е, когато данните

се бекъпват към услуга или съоръжение с дискови масиви през интернет. С правилните акредитиви за вписване, този бекъп може в последствие да се достъпи или възстанови от, който и да е компютър с достъп до интернет.

⁂ **Предимства** – предлага същите предимства като offsite бекъпа; предоставя възможност за лесно свързване и достъпване на бекъпа само с връзка към интернет; информацията е репликирана през няколко устройства за съхранение и обикновено използващи няколко интернет корекции, така че системата не е с една единствена възможност за грешки във връзката; когато услугата е предлагана от добър комерсиален дейта център, услугата е управлявана и защитата не е паралелна.

⁂ **Недостатъци** – отново по-скъпи от локалните бекъпи; може да изисква повече време за съхраняване и възстановяване.

# Архивиране/Data archiving

* 1. **Определение** – преместване на данни/файлове, които се използват рядко, в евтини и защитени хранилища, за да може да се освободи дисково пространство (*фиг. 29 в приложение*). Процесът е важна част от стратегията за управление на данните. Преместените данни са такива, че няма да се променят активно и е възможно да не се използват изобщо. В дигиталният свят, архивирането означава компресиране и въвеждане в архивни файлови формати на вече неизползваната регулярно информация и данни. По този начин се постигат следните цели:

1. съществуващите архивни единици се записват в сигурно хранилище.
2. по този начин се освобождава дисково/сървърно пространство за нови данни.

Има и строго регулирани индустрии, с правила, които задължават архивите да се съхраняват и поддържат за определен период от време. Някои от тях са банкирането, сигурността, здравеопазването и легализиращите институции. Дори ако потребителят не е от горе изброените, пак има случаи в които архива би бил полезен. Примерно стари снимки, видеа или филми, важни документи, или т.н., които биха били желани за съхранение за дълъг период от време и няма да изискват променяне.

* 1. **Начини на реализация** – архивирането на данни може да се реализира по различни начини. Най-елементарният е, съдържащите се в дадена папка данни да бъдат добавени към архив (формати: \*ZIP., 7Z, RAR, TAR, и др.). Създаването на такъв архив, който във файловия мениджър се разпознава като един-единствен файл има редица предимства. Най-напред той компресира съществуващите файлове и значително редуцира размера на заеманото дисково пространство. Освен това, трансферът на този единичен файл е значително по-бърз процес от копирането към външен носител или облачно пространство на множеството файлове от директорията, която се архивира. Тези начини за архивиране са подходящи за малки сървъри, малки фирми и при домашна употреба. Архивирането на данни в големи корпорации, фирми и учреждения изисква ползването на специализирани системи. Това може да са както платени софтуерни пакети, които осигуряват реализирането на архивирането, така и собствено създадени софтуерни конфигурации, които да гарантират архивирането на потребителските данни. Нещо повече, тези процедури могат да бъдат автоматизирани с използване на скриптове и серии от команди, изпълнявани в конзола, които осигуряват стандартизирани архивни процедури за защита на не-регулярно използвани данни.

# 7.4. Локации за съхранение на архива

Тъй като архивираните данни не се използват, масово се съхраняват в режим само за четене, така че да не могат да бъдат променяни.

* **Прикрепени мрежови дискове или такива, прикрепени чрез USB връзка** – често използвани,

но техен недостатък е цената. Мрежовото съхранение изисква недвижими имоти за разполагане и скъп хардуер за защита и поддръжка. Мрежовите дискове предлагат сигурни архиви от данни, които са лесно достъпни, ако организацията или разследващите някога се нуждаят от достъп до тях.

* **Съхранение в облак** – има предимствата на достъпността и ниските разходи, но скоростта зависи от пропускателната способност и скоростта на мрежата на организацията. Много организации са преминали към съхранение в облак заради удобството и икономиите, но все още организацията носи отговорност за запазване на сигурността на данните.

Препоръчва се **използването на софтуер за автоматизиране на процеса**. Функциите и възможностите, предлагани от софтуера за архивиране, зависят от доставчика, но повечето имат стандартни функции за всяка платформа. Администраторът конфигурира времето, местоположението и данните, които трябва да бъдат архивирани, а софтуерът прави останалото. Трябва да се създаде политика за архивиране, за да се определят правилата за преместване на данните. С помощта на политиките за архивиране администраторът гарантира, че данните, преместени на мястото за съхранение, следват правилните регулаторни стандарти и изисквания.

* 1. **Разлики между Backup и Архивиране** – (*таблица 2 в приложение)*

# ЧЕТВЪРТА ЧАСТ ПРАКТИЧЕСКА ПОСТАНОВКА

1. **Изграждане на сървър под операционна среда Windows Server 2019**

# Избор на операционна среда

Сървър може да бъде „вдигнат“ под различни операционни системи като: Linux Ubuntu Server, Red Hat Enterprise Linux, CentOS, включително и десктоп версии могат да бъдат използвани.

Основната причината за избор на Windows за целите на дипломната работа е добре познатият интерфейс. Друга причина, която може да се посочи е, че 73% от компютърните потребители използват някоя от версиите на Windows (*препратка 5 в приложение*). Хубаво е да се спомене, че повечето професионалисти в сферата предпочитат да работят на Linux базирани операционни среди, заради това, че те са отворен код и са безплатни.

# Тип на сървъра, използван за практическата задача

Както беше разгледано в **II.1.7. Типове сървъри според големината/натоварването им**, съществуват 3 големи групи сървъри – бизнес клас, малки бизнес/домашни сървъри и мобилни. Използваният за задачата сървър, спада към втората група – малки бизнес/домашни сървъри.

Машината не е специализиран сървър, а е компютър, който ще играе ролята на сървър. Има сравнително добри характеристики и има потенциалът да върши доста полезна работа.

# Минимални изисквания към компютърния хардуер/System requirements:

**Процесор** – 1.4 GHz 64-bit; **RAM памет** – 512 MB; **дисково пространство** – 32 GB; **мрежа** – Gigabit (10/100/1000baseT) Ethernet adapter; **оптично устройство** – DVD drive (ако ОС ще се инсталира от дисково устройство); **видео** – Super VGA (1024 **x** 768) or higher-resolution (избирателно); клавиатура и мишка (избирателни); **интернет** – Broadband access (optional).

# Стъпки за инсталация на Windows Server 2019

Изтегляне на лицензиран или безплатен за 180 дена/free trial Windows Server 2019 (*препратка 6 в приложение*). Чрез софтуера на фирма Ventoy, се форматира на флаш USB устройството в bootable flash drive (*препратка 7 в приложение*) и към него се прехвърля ISO файлът с Windows Server 2019. Поставяне на флашката/диска и стартиране на машината. Ако се прави на VirtualBox, KVM и VMware трябва само да прикачат ISO файла по време на създаването на виртуална машина и да следват стъпките за инсталация.

1. На първия екран, избиране на език за инсталиране, време, клавиатурна подредба и кликване на "Next".
2. Стартиране на инсталацията, като се избере “Install now”. Setup-а ще започне след малко.
3. Избиране на Windows Server 2019 Standard Evaluation (Desktop experience) за инсталиране и потвърждаване с “Next” (*фиг. 30 в приложение*).
4. Прочитане и потвърждаване на License terms, като се отбележи квадратчето “I accept the license terms”.
5. На следващия прозорец, трябва да се избере между Upgrade или Custom (*фиг. 31 в приложение*). Първият вариант ще запази файловете, настройките и приложенията на предишния Windows (ако е имало преди това), докато при Custom всичко ще бъде изтрито и ще се наложи да се инсталира и персонализира наново. Втората опция е по-подходяща, ако се инсталира на машина, която до момента не е имала операционна система Windows.
6. Следващата стъпка са настройването на партишъните. Трябва задължително да се зададе на коя част на диска ще бъде Windows server-а, докато другите настройки са си според самия потребител (*фиг. 32 в приложение*).
7. Инсталацията ще започне. Изчакване докато приключи.
8. Системата най-вероятно сама ще се рестартира/reboot-не. Задаване на администраторска парола, когато зареди новият екран и кликване на бутона Finish.
9. За логване с администраторски юзър/user използване на комбинацията Ctrl + Alt + Del. Въвеждане на парола.
10. След правилно въведена парола, би трябвало да зареди десктопа и на него да излезе Server manager (*фиг. 33 в приложение*).
11. За проверка: Windows бутон – Settings – System – About – Edition (*препратка 8 в приложение*).

# Изграждане на софтуерен RAID масив под Windows Server 2019

* 1. **Характеристики на машината:**

*Компютърна система в кабинет 5.4 (компютър Nº3) е със следните характеристики:*

⁂ ***Дънна платка***: H81M-DS2

⁂ ***Производител на дънната платка***: Gigabyte Technology Co., Ltd.

⁂ ***Процесор***: Intel Core i5-4460 CPU @ 3.20 GHz

⁂ ***RAM памет***: 8,00 GB

⁂ ***Име на инсталираната операционната система***: Microsoft Windows Server 2019

# Стъпки за свързване на два хард диска в технология RAID 1

* + - **Хардуерна част** – спиране на захранването и отваряне на компютърната кутия. Поставяне на електростатична гривна и монтиране на двата хард диска в предназначеното за тях пространство. Много е важно двата хард диска да са с еднакъв обем и с един и същ интерфейс. В този случай това е SATA. Включване на хард дисковете към захранване и затваряне на компютърната кутия (*фиг. 34 в приложение*). Пускане на захранването и стартиране на машината.
    - **Софтуерна част** – Windows Server има вградена функционалност, за настройване на софтуерен RAID без допълнителни инструменти. Това улеснява превръщането на съществуващите резервни твърди дискове в свързан RAID масив.

1. Архивиране на информацията, която се намира на дисковете. Дори да не е необходимо да се форматира диска е хубаво данните да ги има като копие. Тази стъпка не е необходима, ако дисковете са нови.
2. Десен клавиш на Windows менюто и отваряне на Disk management. Кликване с десен бутон върху един от volume-ите на диска и селектиране на “New mirror volume” (*фиг. 35 в приложение*).
3. Ще излезе Pop up прозорец – “welcome to the New Mirrored Volume Wizard”. Потвърждаване с “Next”.

При “select the amount of space in MB”, се избира дисковото пространство което ще бъде включено от избрания диск (може и целият да бъде избран и по принцип така се прави) за RAID 1 (*фиг. 36 в приложение*).

1. Избиране на другия диск, който е със същия капацитет и интерфейс и кликване на “Add” (*фиг. 37 в приложение*). Автоматично ще му се зададе избрания преди това размер (който ще бъде ползван за RAID-а).
2. Избиране на буква с която ще е озаглавен и потвърждаване с “Next”.

На следващата стъпка може да се зададе име на volume-а/Volume label (например MIRRORED\_VOL). Избирателно селектване на “Perform a quick format” (*фиг. 38 в приложение*). Потвърждаване с “Next” и на последната стъпка “Finish”.

1. След като процеса завърши, би трябвало двата селектирани диска да сменят цвета си на червен или ако е зададен част от дисковете за RAID-а, само част от диска ще засвети в червено (фиг. 39 в приложение).
2. За проверка: File manager – this PC и търсим името на volume-a или буквата му.
3. Ако трябва да се премахне Mirror-a, десен клавиш на един от тях и селектиране на “Remove

mirror”. Конкретизиране на кой от двата диска да бъде премахнат и потвърждаване с “Remove mirror” – “Yes” (*фиг. 40 в приложение*). (*препратка 9 в приложение)*

Следвайки тези стъпки се конфигурира сървър с операционна система Windows Server 2019 с изграден RAID масив 1.

# ИЗВОДИ, ОБОБЩЕНИЕ И ЗАКЛЮЧЕНИЕ ИЗВОДИ:

След направеното разглеждане на развитието на **запомнящите устройства** през годините, установяваме, че двата основни носителя на информация, използвани в сървърни конфигурации са **хард дискове** и **солид стейт дискове**. Обикновено SSD-то се използва за операционната среда, а хард диска е основната памет която се използва. Това се дължи на факта, че бързодействието на SSD превишава това на хард диска, но ако се гледа колко презаписвания на информация могат да се правят – хард диска е правилният избор. **Флопи диск** и **CD/DVD-та** могат да се използват за архивиране на данни, в случай че сървъра има необходимите четци (с дискове може да се инсталира и операционна система), но реално те са вече отживелица.

След като се запознаем със същността на **сървърите**, стигаме до заключението, че те се делят на 2 големи групи – хардуерни и софтуерни. Хардуерният сървър е нормален, докато виртуалният се позиционира върху хардуерен – точно както при PC-тата, виртуалната машина се изгражда софтуерно върху компютъра. Също така, сървърите могат да се подразделят на такива, които имат конкретна задача и на такива, които извършват няколко функции едновременно. Според това, под какво натоварване са подложени, има 3 основни групи сървъри – бизнес клас, обслужващи малка фирма/домашни сървъри и мобилни. Важно да се спомене е, че масово сървърите работят непрестанно. Това е така, защото други потребители зависят от него и дори ако бъде спрян за малък период от време, това може да нанесе щети както финансово, така и репутационно. За правилен избор на сървър, трябва да се прецени каква ще е основната му бъдеща функция.

# ОБОБЩЕНИЕ:

Ако е необходимо голямо количество дисково пространство или за даден сървър или за по-сериозен потребител, ще трябва да се конфигурират повече от един хард диск. Съществуват няколко метода

– **JBOD**, **SPAN/BIG**, **MAID**, но най-използваният е **RAID**. RAID не бива да се използва като резервно копие на данните, тъй като технологията осигурява защита при повреда на някой от дисковете, но не предпазва от злонамерена дейност в уеб пространството, хакери и други. Предназначението му е да подобри производителността и да намали риска от загуба на данни.

Заплахите за сигурността и методите за защита са много обсъждана тема в съвремието, което се дължи на все по-голямото количество потребители, присъединяващи се към глобалната мрежа всеки ден. Тъй като новите потребители не са запознати с дебнещите ги заплахи, те са уязвими. Също така, хората с висока позиция в обществото, също са рискови както от материална гледна точка, така и при атака могат да загубят чувствителни/компрометиращи данни.

Главните **заплахи за сигурността** са зловреден софтуер, техническа неизправност, нелоялен

служител, човешка грешка и външни атаки, като се има предвид, че съществуват още много видове и подвидове. Най-важните методи за превенция са честата актуализация на софтуера и операционната система, ограничаване на достъпа до чувствителни данни, използване на VPN, защитаване на данните чрез използване на криптиране и пароли и др. Подробно разгледани методи за защита бяха **защитната стена**, **антивирусният софтуер**, **криптирането, бекъпа** и **архивирането**.

# ЗАКЛЮЧЕНИЕ:

Така разработеният дипломен проект, може да влезне като учебно-методично ръководство в професионалните предмети изучавани в специалностите Компютърна техника и технологии и Компютърни мрежи. Разработеният проект може да се ползва по предметите Запомнящи и периферни устройства, Компютърни мрежи, както и по Софтуер и Операционни среди. Приложим е, както за теоретична подготовка, така и за практическа. Изграждането на софтуерен RAID е много подходящо упражнение за двете специалности по КТТ.

# ИЗТОЧНИЦИ

**Теоретична част:**

https://[www.lifewire.com/what-is-a-floppy-drive-2618151](http://www.lifewire.com/what-is-a-floppy-drive-2618151) https://computer.howstuffworks.com/floppy-disk-drive.htm https://ssd.eff.org/bg/tech/encryption https://ssd.eff.org/bg/tech/disk-encryption https://en.wikipedia.org/wiki/Norton\_AntiVirus https://[www.computerhope.com/jargon/s/server.htm](http://www.computerhope.com/jargon/s/server.htm) https://[www.lifewire.com/servers-in-computer-networking-817380](http://www.lifewire.com/servers-in-computer-networking-817380)

https://[www.cloudsavvyit.com/3590/which-type-of-raid-should-you-use-for-your-servers/](http://www.cloudsavvyit.com/3590/which-type-of-raid-should-you-use-for-your-servers/) https://en.wikipedia.org/wiki/Server\_(computing)

https://youtu.be/UjCDWCeHCzY <http://tuj.asenevtsi.com/CN/N084.htm>

https://liptrade.eu/%D0%BA%D0%B0%D0%BA%D0%B2%D0%BE-%D0%B5-

%D0%B0%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81-

%D0%B8%D0%BC%D0%B0%D0%BC%D0%B5-%D0%BB%D0%B8-

%D0%BD%D1%83%D0%B6%D0%B4%D0%B0-%D0%BE%D1%82-%D1%82%D0%B0%D0%B7/

https://[www.investopedia.com/terms/e/encryption.asp](http://www.investopedia.com/terms/e/encryption.asp) https://[www.cloudflare.com/learning/ssl/what-is-encryption/](http://www.cloudflare.com/learning/ssl/what-is-encryption/) https://[www.techtarget.com/searchsecurity/definition/encryption](http://www.techtarget.com/searchsecurity/definition/encryption) https://[www.kaspersky.com/resource-center/definitions/encryption.](http://www.kaspersky.com/resource-center/definitions/encryption) https://[www.cisco.com/c/en/us/products/security/encryption-explained.html](http://www.cisco.com/c/en/us/products/security/encryption-explained.html) https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

https://[www.techtarget.com/searchdatabackup/feature/Full-incremental-or-differential-How-to-choose-the-](http://www.techtarget.com/searchdatabackup/feature/Full-incremental-or-differential-How-to-choose-the-) correct-backup-type

https://parablu.com/demystifying-data-backups-types-of-backups/ https://[www.welivesecurity.com/2019/05/10/types-backup-mistakes-avoid/](http://www.welivesecurity.com/2019/05/10/types-backup-mistakes-avoid/) https://[www.acronis.com/en-us/articles/data-backup/](http://www.acronis.com/en-us/articles/data-backup/) https://cloudian.com/guides/data-backup/data-backup-in-depth/ https://[www.sciencedirect.com/topics/engineering/floppy-disk](http://www.sciencedirect.com/topics/engineering/floppy-disk)

https://[www.serverwatch.com/guides/what-is-a-server/](http://www.serverwatch.com/guides/what-is-a-server/) https://bg.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%

83%D1%81%D0%B5%D0%BD\_%D1%81%D0%BE%D1%84%D1%82%D1%83%D0%B5%D1%80

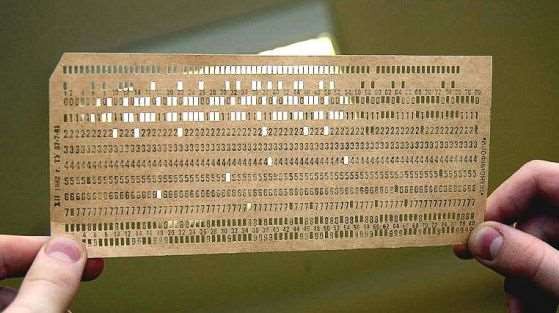
https://[www.ironmountain.com/blogs/2020/5-major-differences-between-backup-vs-archive](http://www.ironmountain.com/blogs/2020/5-major-differences-between-backup-vs-archive) https://[www.sciencedirect.com/topics/computer-science/asymmetric-cryptography](http://www.sciencedirect.com/topics/computer-science/asymmetric-cryptography) https://[www.webmasterview.com/2011/03/server-security-threats/](http://www.webmasterview.com/2011/03/server-security-threats/) https://usa.kaspersky.com/resource-center/definitions/firewall

# Практическа част:

https://bg.if-koubou.com/articles/how-to/how-to-create-a-software-raid-array-in-windows-7.html https://computingforgeeks.com/install-windows-server-2019/

https://youtu.be/RkZjx-1cVCM https://youtu.be/SwicvNPg4QU

# ПРИЛОЖЕНИE

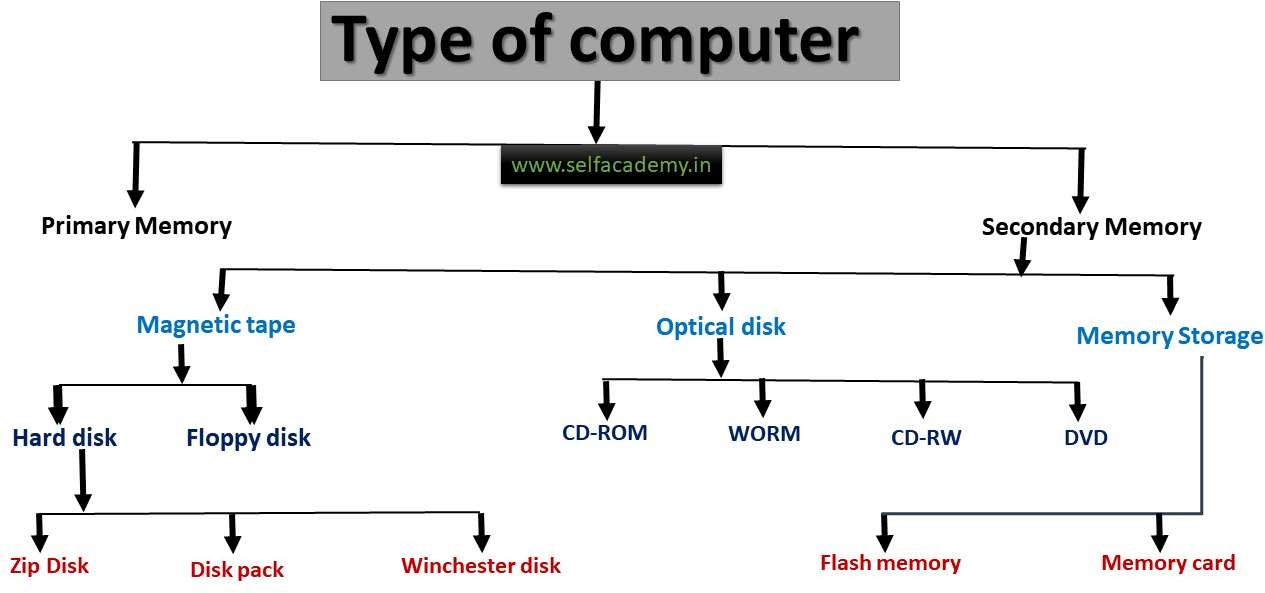


**Фиг. 1** – Перфокарта

***Препратка 1*** – https://[www.scienceandindustrymuseum.org.uk/objects-and-stories/jacquard-loom](http://www.scienceandindustrymuseum.org.uk/objects-and-stories/jacquard-loom)



**Фиг. 2** – Магнитни ленти

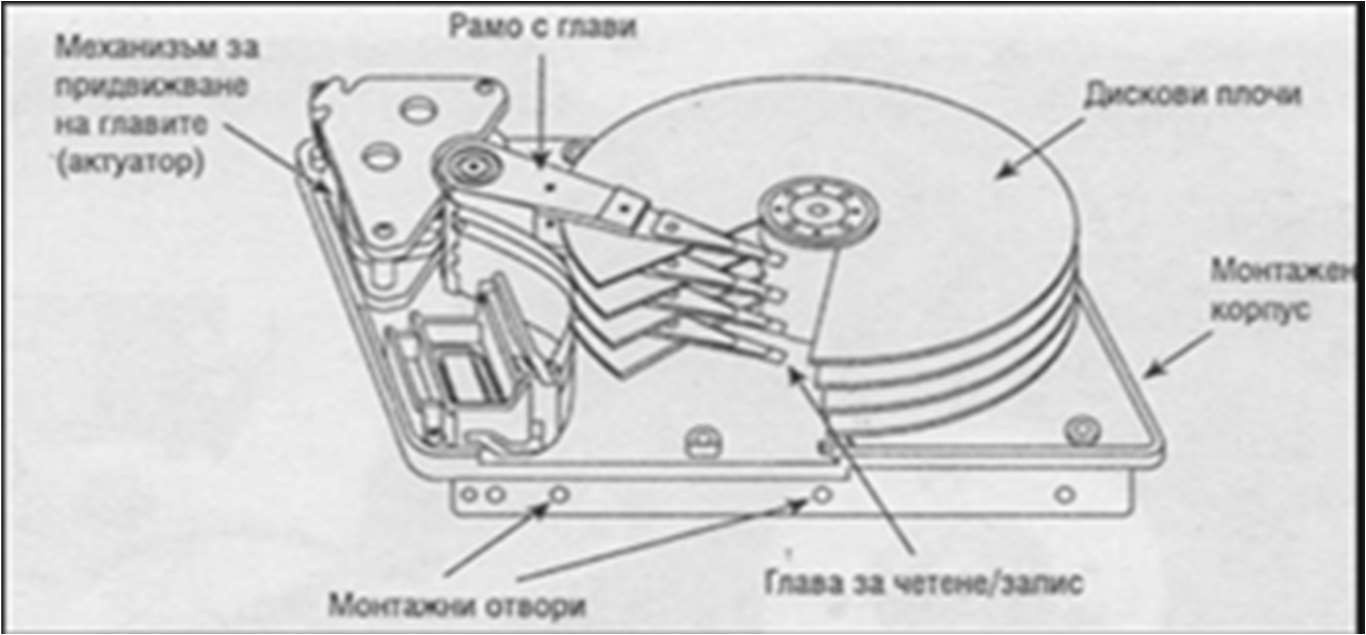


**Фиг. 3** – Класификация на запомнящите устройства

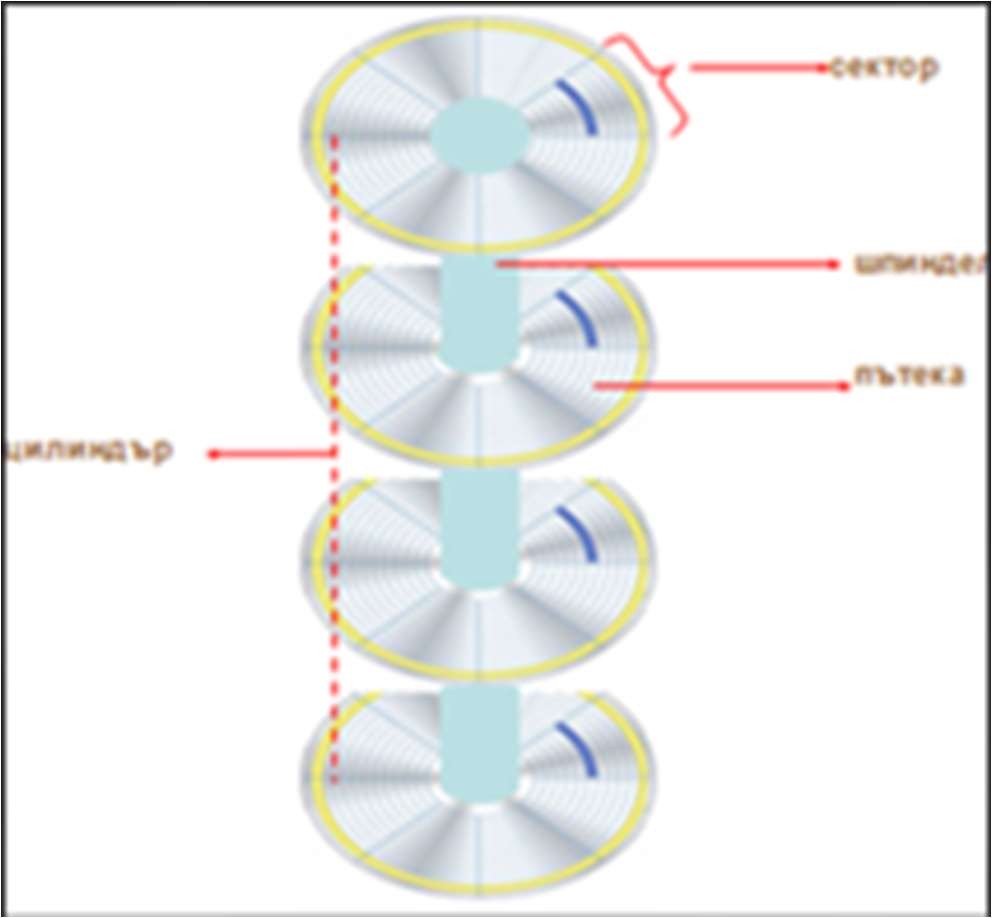


**Фиг. 4** – Флопи диск – FDD



**Фиг. 5** – Отворен хард диск

**Фиг. 6** – Части на хард диск



**Фиг. 7** – Цилиндър, сектор, шпиндел и пътека в хард диск



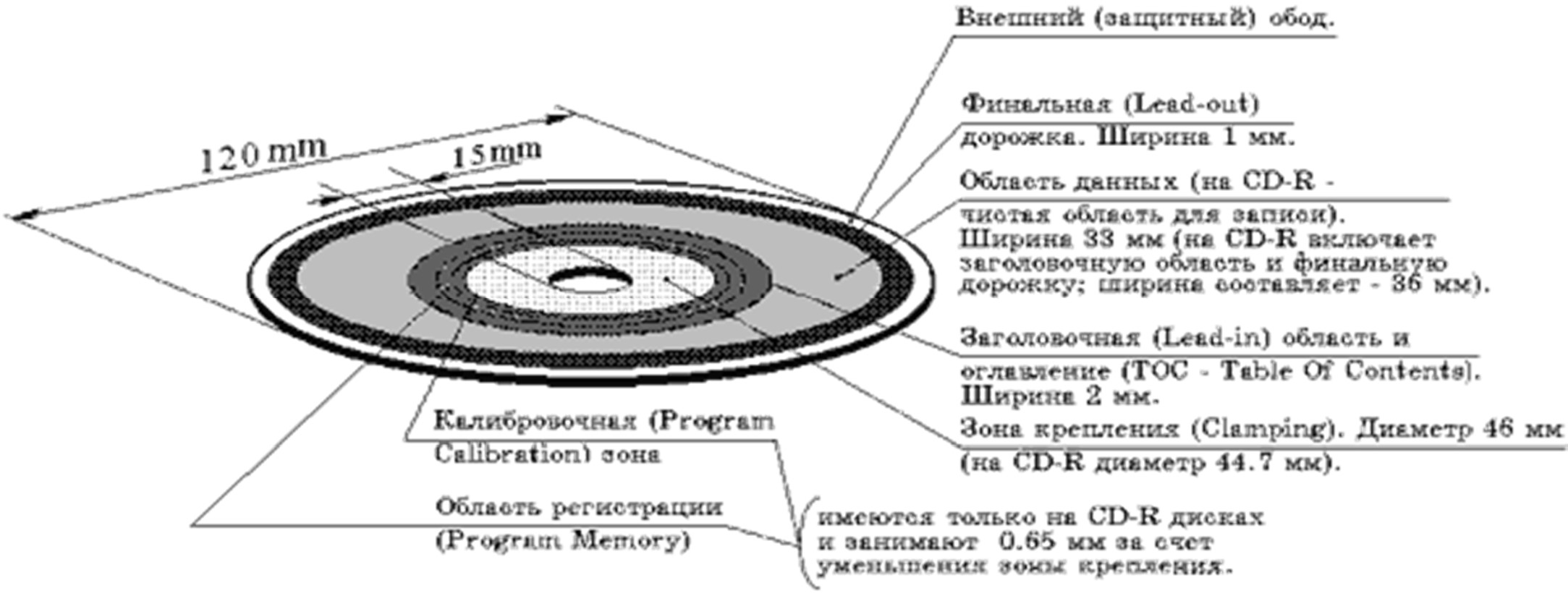
**Фиг. 8** – Samsung солид стейд драйв

|  |  |
| --- | --- |
| **HDD** | **SSD** |
| Принцип на действие – магнитен запис и четене на информация | Принцип на действие – записва и чете на принципа на флаш паметите (чрез активиране и деактивиране на клетки с  внезапни спирания на захранването) |
| Еднаква скорост на въртене на диска | Няма механични части |
| Тъй като външните писти са малко по- дълги от вътрешните има по-голямо разстояние между битовете от тези във  вътрешните писти | Клетките в едно SSD за равномерно разпределени. |
| Време на достъп (random access time) –  от 5 до 15 ms. | Време на достъп (random access time) – от  25 до 100 μs. |
| Дисковият пакет не се сменя и е затворен  заедно с блока на магнитните глави в херметична кутия | Платката с чиповете за памет е опакована, но не в херметична кутия |
| Съхранява се само цифрова  информация. | Съхранява се само цифрова информация. |

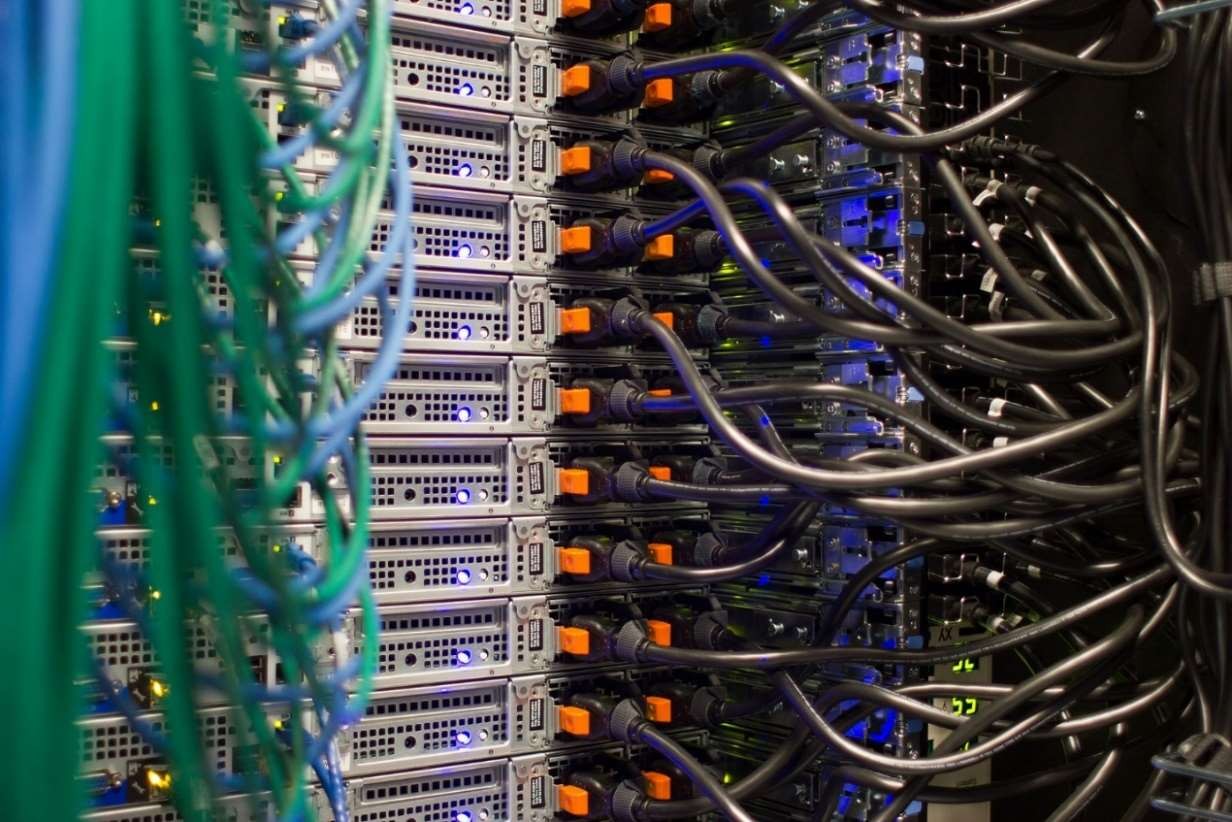
***Таблица 1*** – Съпоставителна таблица на хард диск и солид стейд драйв



**Фиг. 9** – Оптични дискове



**Фиг. 10** – Конструкция на диск



**Фиг. 11** – Сървър в работещо състояние



**Фиг. 12** – Отворен сървър

# Архитектура на сървъра

⁂ Паралелна компютърна архитектура. Операционната система работеща с четири и повече процесора ще балансира товара на задачата така, че да се постига добра производителност на сървъра.

⁂ Код за коригиране на грешките /ЕСС/ подсилва сигурността на сървъра и целостта на данните.

⁂ Кеширането на данните в паметта оптимизира производителността на сървъра.

⁂ Два мрежови адаптера позволяват сегментиране товара на клиентите на сървъра. Софтуерът обединява двата порта в един. Вторият адаптер служи за осигуряване на по-висока честотна лента или като резервен.

⁂ Смяна на дисковете по време на работа. Използване на технологията RAID Level 5.

⁂ Връзка към устройства за бързо съхранение на данни

⁂ Непрекъсваеми по време на работа захранвания с двойни мрежови кабели и два допълнителни вентилатора.

***Приложение 1*** – Архитектура на сървъра

* **Уеб сървър/Web server** – компютърна програма, която обслужва заявени HTML страници или файлове. В този случай уеб браузърът действа като клиент – Internet Explorer, Chrome, Firefox, Opera или Safari. Използват се за много задачи в допълнение към доставянето на прост текст и изображения, например за качване и архивиране на файлове онлайн чрез услуга за съхранение в облак или онлайн услуга за архивиране.
* **Сървър за приложения** – програма в компютър в разпределена мрежа, която осигурява бизнес логиката за дадена програма за приложения. Правят данните и сървърната част на приложенията от типа клиент/сървър достъпни за клиентите. При сървъра за приложения базата данни се намира на сървъра, а на клиентският компютър чрез форми се попълват данни или чрез заявки се извлича информация.
* **Пощенски сървър** – управлява електронните съобщения между потребителите на мрежата. Получава входящи имейли от местни потребители – хора в рамките на един и същи домейн – и отдалечени изпращачи и препраща изходящи имейли за доставка.
* **Файлов сървър/File server** – компютър, който отговаря за централното съхранение и управление на файлове с данни, така че други компютри в същата мрежа да имат достъп до тях. Синхронизира достъпа до общите ресурси.
* **Упълномощен сървър/Proxy сървър** – софтуер, който действа като посредник между крайно устройство, например компютър, и друг сървър, от който потребителят или клиентът заявява услуга.
* **Виртуален сървър/Virtual server** – програма, работеща на споделен сървър, която е конфигурирана по такъв начин, че за всеки потребител изглежда, че има пълен контрол върху сървъра.
* **Блейд сървър/Blade server** – сървърно шаси, в което са разположени множество тънки модулни електронни платки, известни като сървърни блейдове. Всеки блейд е самостоятелен сървър, често посветен на едно-единствено приложение.
* **Сървър за политики/Policy server** – компонент за сигурност на мрежа, базирана на политики, който предоставя услуги за оторизация и улеснява проследяването и контрола на файловете.
* **Сървър за бази данни**/**Database server** – този сървър отговаря за хостването на една или повече бази данни. Клиентските приложения изпълняват заявки към базата данни, които извличат данни от или записват данни в базата данни, която се хоства на сървъра.
* **Сървър за печат/Print server** – този сървър осигурява на потребителите достъп до един или повече мрежови принтери – или устройства за печат, както ги наричат някои доставчици на сървъри. Сървърът за печат действа като опашка за заданията за печат, които потребителите подават. Някои сървъри за печат могат да приоритизират задачите в опашката за печат въз основа на типа на задачата или на това кой е подал задачата за печат.
* **FTP сървър** – FTP сървърите преместват файлове чрез инструменти на протокола за прехвърляне на файлове. FTP сървърите са достъпни от разстояние с помощта на FTP клиентски програми, които се свързват с файловия дял на сървъра чрез вградените FTP възможности на сървъра или със специална FTP сървърна програма.
* **Сървър за идентичност**/**User identity server** – сървърите за идентичност поддържат влизания и роли за сигурност за оторизирани потребители.
* **Сървър за ІР адресиране**/**DNS/Domain Name Server** – извършва услуги по управление на ІР адреси
* **Сървър, осъществяващ защитната стена** – сървърът може да има три адаптера:

⁂ за връзка с Интернет

⁂ създава защитна стена и пълен контрол върху маршрутизирането на постъпващите пакети

⁂ адаптер за локална мрежа, който дава възможност на потребителите да се включват в други корпоративни локални мрежи

⁂ адаптер за защитаваната LAN.

* **Факс сървър** – управлява трафика на факсове към и от мрежата. Може чрез обществената телефонна мрежа да предава факсове към факс апарати.
* **Сървъри за директорийни услуги** – позволяват на потребителите да локализират, съхраняват и защитават информацията в мрежата.
* **Други сървъри** – колкото функции изпълнява мрежата, толкова вида сървъри могат да бъдат създадени. Това е въпрос на проектиране, оптимизация на структурата и естествено пари.
* **Общи видове сървъри** – докато някои специализирани сървъри се фокусират върху една функция, като например сървър за печат или сървър за бази данни, някои реализации използват един сървър за множество цели. Голяма мрежа с общо предназначение, която поддържа средна по големина компания, вероятно разполага с няколко вида сървъри, включително: стотици специализирани типове сървъри поддържат компютърни мрежи. Освен обичайните корпоративни типове, домашните потребители често си взаимодействат със сървъри за онлайн игри, чат сървъри, сървъри за аудио и видео стрийминг и др. Някои сървъри съществуват с конкретна цел, но не е задължително да се взаимодейства с тях по някакъв значим начин. Пример за това са DNS сървърите и прокси сървърите.
* **Видове мрежови сървъри** – в много мрежи в интернет се използва мрежов модел клиент-сървър, който интегрира уебсайтове и комуникационни услуги. Алтернативният модел, наречен **peer-to-peer мрежа**, позволява на всички устройства в мрежата да функционират като сървър или клиент при необходимост. Равнопоставените мрежи предлагат по-голяма степен на поверителност, тъй като комуникацията между компютрите е тясно насочена. Въпреки това, отчасти поради ограниченията на честотната лента, повечето реализации на peer-to-peer мрежи не са достатъчно надеждни, за да поддържат големи скокове на трафика.

# Облачен сървър

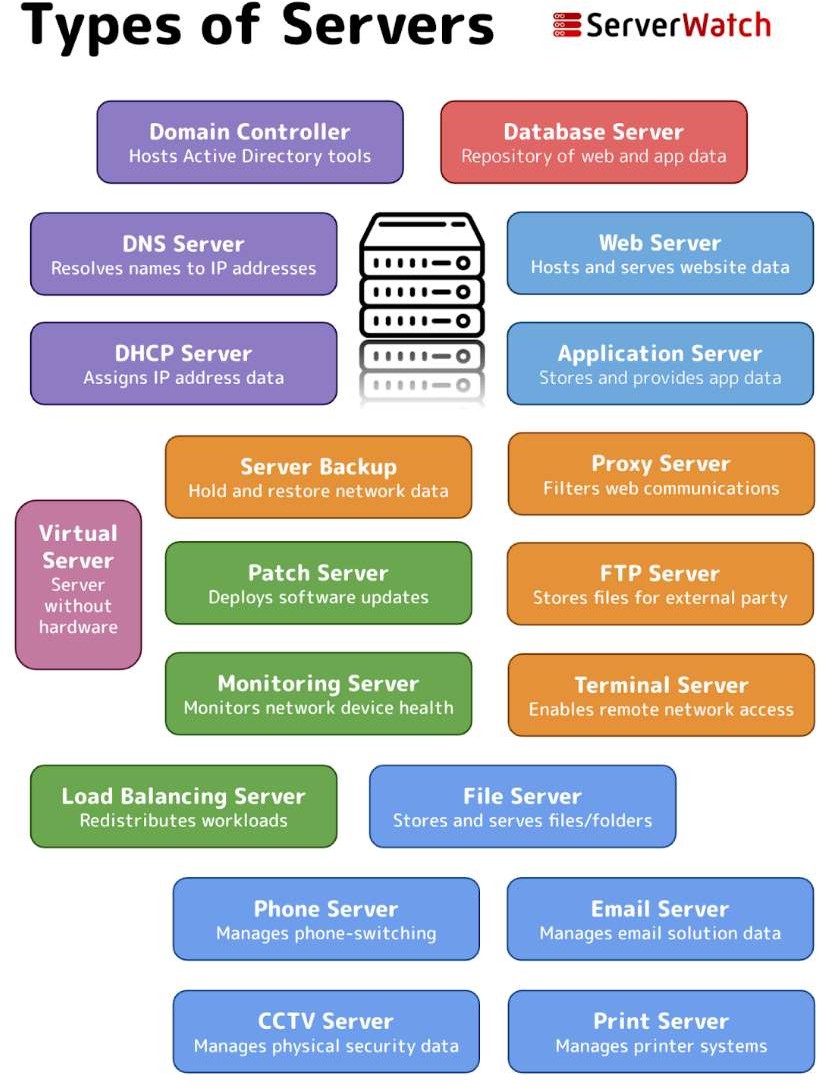
* **Сървър за бази данни**

# Специализиран сървър

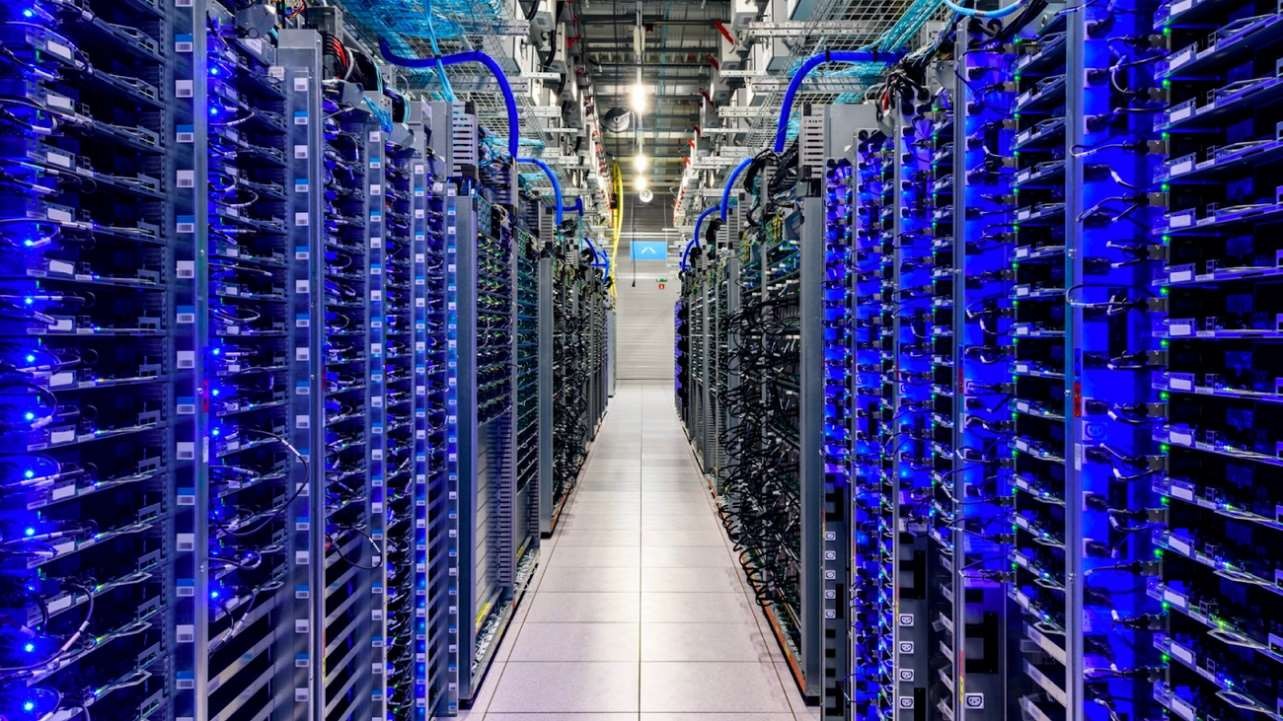
* **Услуга за име на домейн**

# Сървър за печат

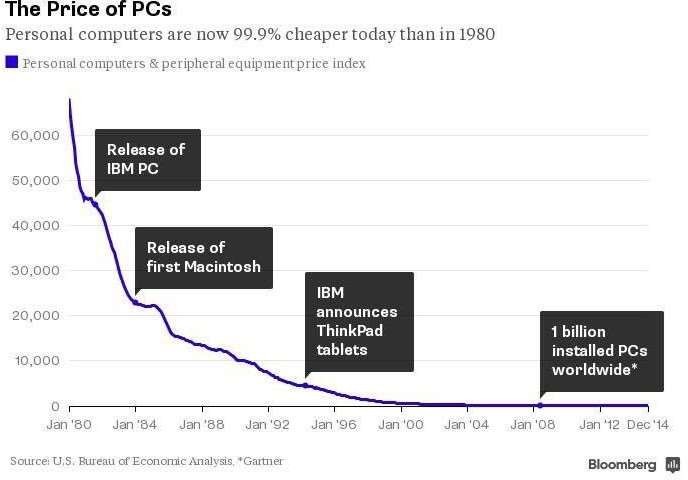
* **Самостоятелен сървър**



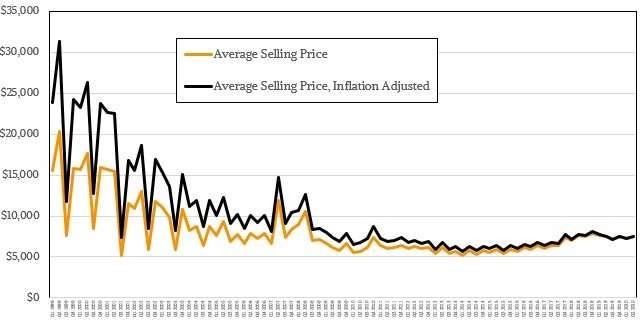
***Приложение 2*** – Видове сървъри, според функцията им на работа



**Фиг. 13 –** Сървърите на Гугъл



**Фиг. 14** – Движение на цените на персонални компютри от 1980 до днес



**Фиг. 15** – Движение на цените на компютърни машини през годините

## Консумация на електроенергия

През 2010 г. центровете за данни (сървъри, охлаждане и друга електрическа инфраструктура) са употребили 1,1-1,5 % от електрическа енергия в света. Според една от оценките, общото потребление на енергия за информационни и комуникационни технологии спестява повече от 5 пъти въглеродния

отпечатък в останалата част на икономиката чрез повишаване на ефективността. Глобалното потребление на енергия се увеличава поради нарастващото търсене на данни и широчина на честотната лента. Съветът за защита на природните ресурси (NRDC) посочва, че през 2013 г. центровете за данни са използвали 91 млрд. киловатчаса (kWh) електрическа енергия, което представлява 3 % от световното потребление на електроенергия. Групите за защита на околната среда поставят акцент върху въглеродните емисии на центровете за данни, тъй като те отделят 200 млн. метрични тона въглероден диоксид годишно.

***Приложение 3*** – Глобална консумация на електроенергия, причинена от сървърите

***Препратка 2*** – Информация относно BIG arrays – https://eshop.macsales.com/shop/hard-drives/sata/RAID-Guide/Learn-About-NRAID

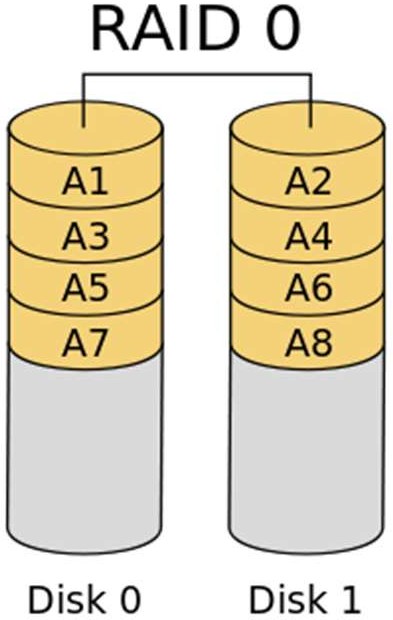
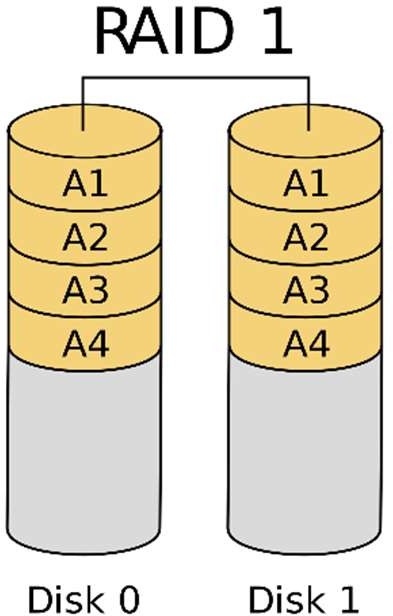
***Препратка 3*** – Информация за BIG и SPAN arrays –

https://en.wikipedia.org/wiki/Non-RAID\_drive\_architectures#Concatenation\_(SPAN,\_BIG)

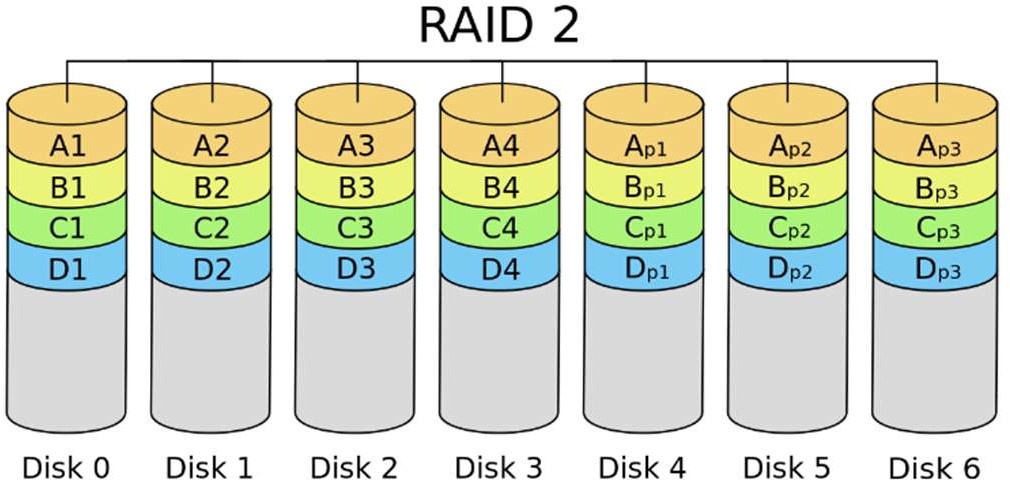


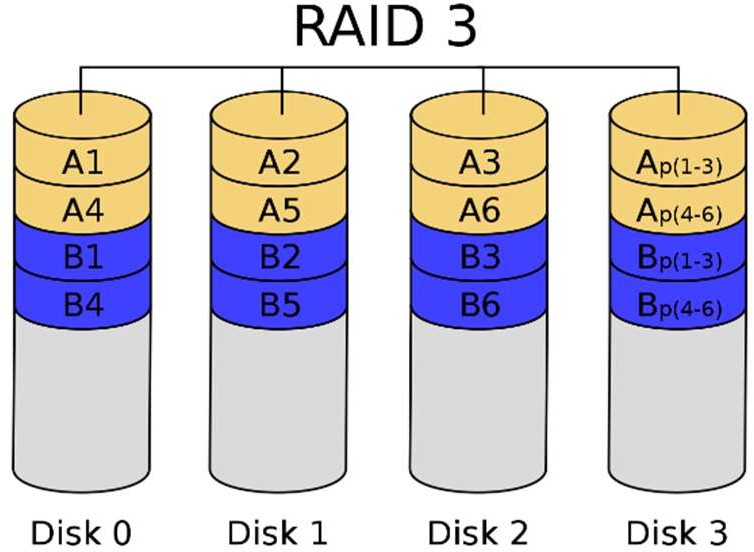
**Фиг. 16** – Няколко хард диска в рак

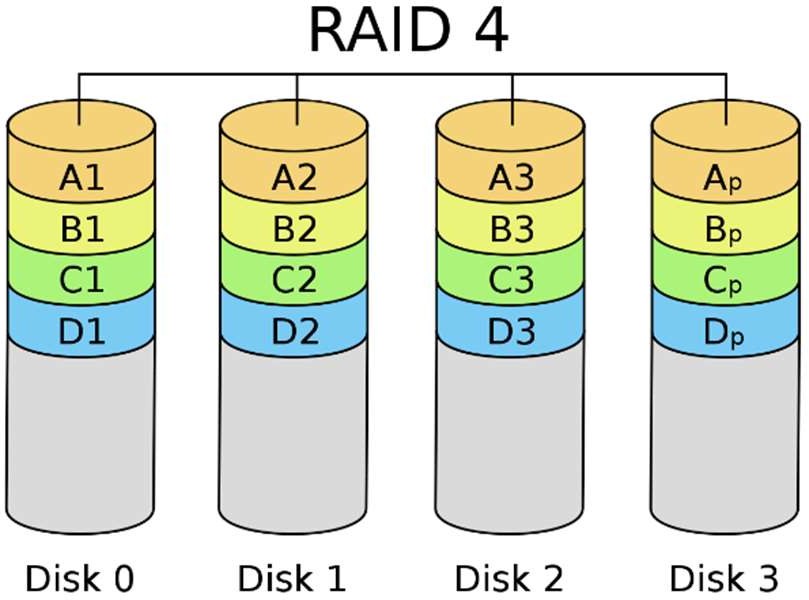
## Стандартни райд нива

* **RAID level 0** – минимум 2 устройства – чист striping; предлага най-добрата производителност, но не позволява защита на данните. при увеличение на дисковете се увеличава бързината на запис/четене няма защита на информацията. Ефективния свободен обем е равен на сбора от капацитетите на инсталираните устройства.
* **RAID level 1** – минимум 2 устройства – опростена защита на данните; изцяло се основава на mirroring. Информацията се копира огледално върху наличните дискове. Тук има подобряване на четенето понеже информацията може да бъде прочетена от две места едновременно. Производителността при запис е същата както при единичен диск. Недостатъкът на това ниво е, че ефективният свободен обем ще бъде двойно по-малък от сбора на инсталираните устройства.
* **RAID level 2** – информацията се разделя на блокове последователно се записват на отделни дискове от масива. За всеки блок е изчислен уникален код за контрол на грешките според битовете за четност. Кодовете се съхраняват на отделни дискови устройства. Необходими са поне 10 диска за данните и поне 4 за кодовете. В случай на отказ на един от дисковете информацията може да бъде възстановена чрез наличните кодове.

Кодовете представляват математичен код за контрол на грешките чрез битове за четност.

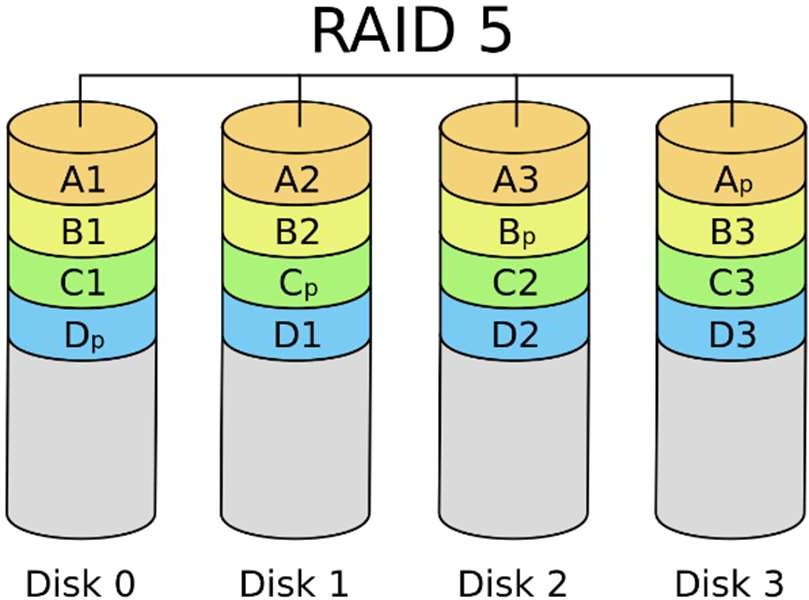


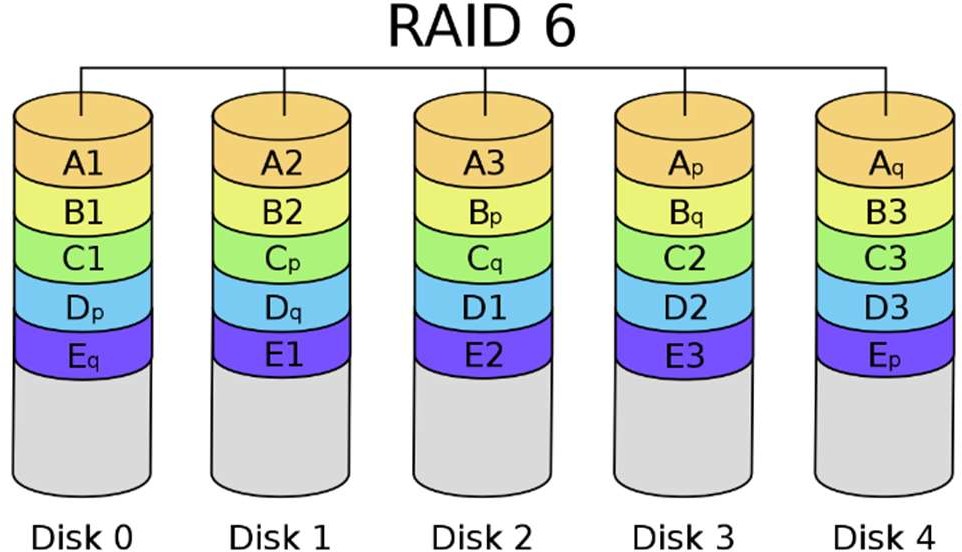
* **RAID level 3** – кодовете са на 1 диск, иначе е същото като RAID level 2. Блоковете от данни се записват последователно по дисковете от масива като един от тях е заделен за съхранение на битове за четност. Надеждността на съхранение на информация е същата като в предходното ниво 2.
* **RAID level 4** – разпределянето на информацията се осъществява като предходните две нива, като отново е предвидено устройство за съхранение на кодовете за четност. За разлика от ниво 2 и 3, където едновременното обработване на две заявки е невъзможно, при ниво 4 подобно ограничение не съществува. Това е предпоставка за по-добра скорост на четене на произволни блокове, в сравнение с тази от предходните две нива. Изискват се поне 3 твърди диска с еднакъв капацитет. Ефективността при това ниво се увеличава с добавяне на повече устройства към масива.



* **RAID level 5** – основава се на разпределянето на блокове от данни с кодове за четност. Както при останалите нива, блоковете от данни се записват последователно в дисковете от масива, но

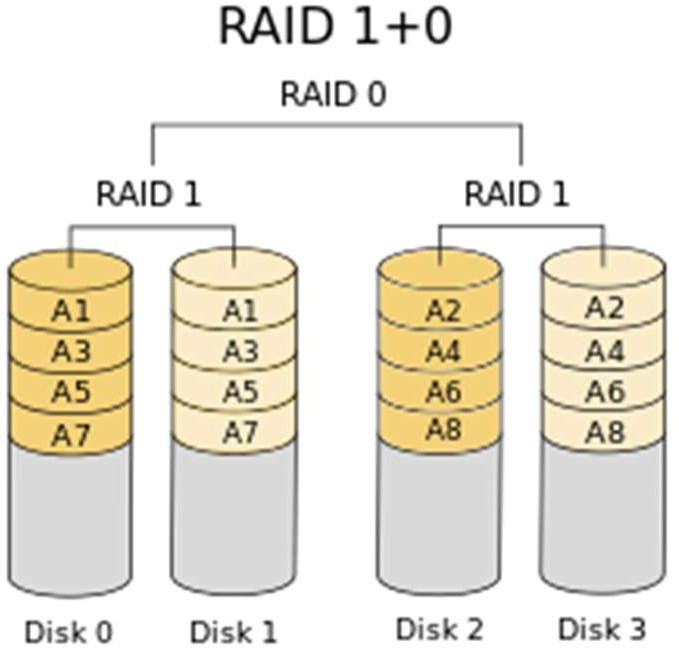
същественото тук, е че кодовете за четност се разпределят последователно по дисковете в масива, а

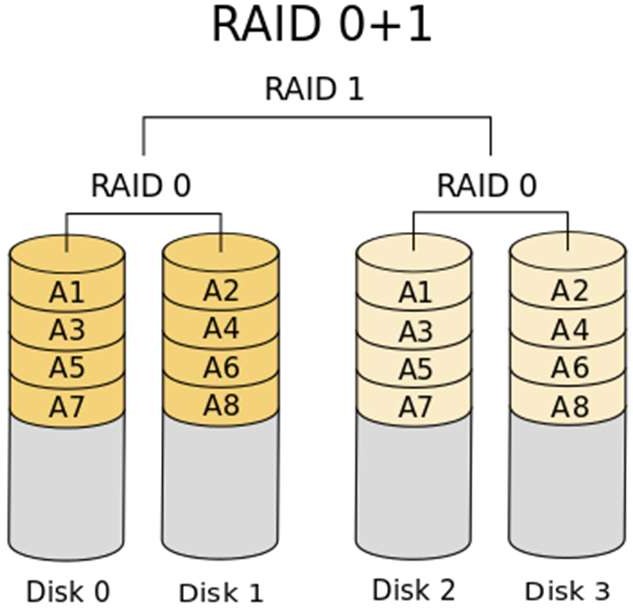
не както при останалите в един единствен диск. При това ниво функционирането се запазва дори при отпадането на един от дисковете. Данните в този случай могат да бъдат възстановени от разпределените битове за четност по останалите дискове. За RAID 5 са необходими минимум 3 диска. Когато един от дисковете отпадне и бива заменен с друг, производителността на масива рязко спада през времето, което е необходимо за възстановяването на отпадналия диск. Това време обикновено е доста дълго, понеже за възстановяването на информацията трябва да бъдат прочетени всички данни от останалите дискове в масива. По времето през което се възстановява изгубеният диск, RAID 5 масива е много податлив към отпадане на втори диск, като в този случай информацията се изгубва безвъзвратно. Това ниво обикновено се приема за неподходящ избор при високи натоварвания при писане.

* **RAID level 6** – като 5, но има двойно разпределение на битовете за четност, има ниска производителност. Те задължително се съхраняват на различни устройства. Така се осигурява функциониране на масива при отпадането на до 2 диска. Минималният брой необходими устройства са четири. Подобен на RAID 5, но при него има двойно разпределяне на битовете за четност. Нивото предлага по-голяма надеждност на съхраняваната информация за сметка на по-малко ефективно пространство и по-ниска производителност в сравнение с RAID 5.

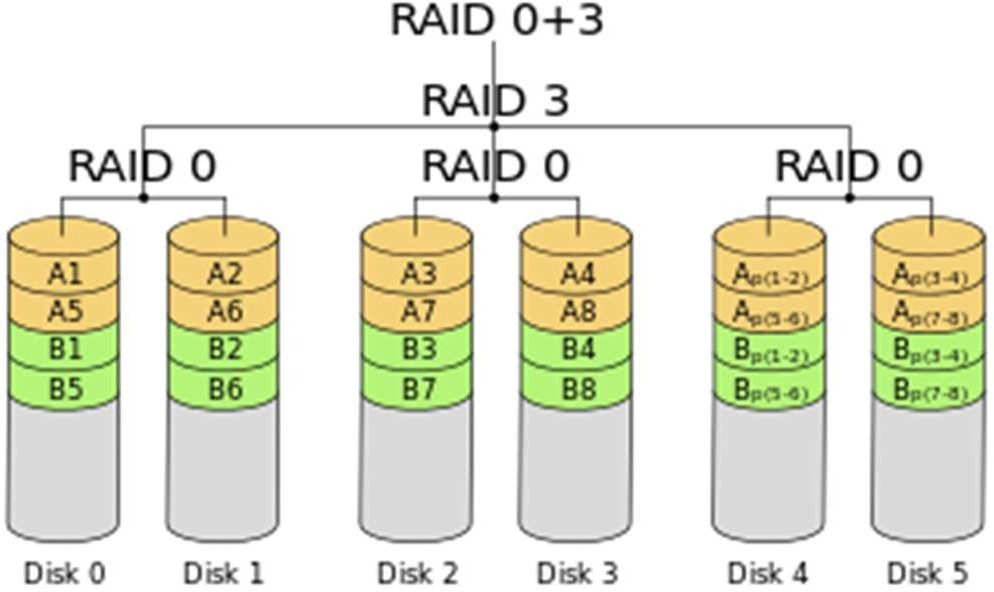
***Приложение 4*** – Стандартни RAID нива

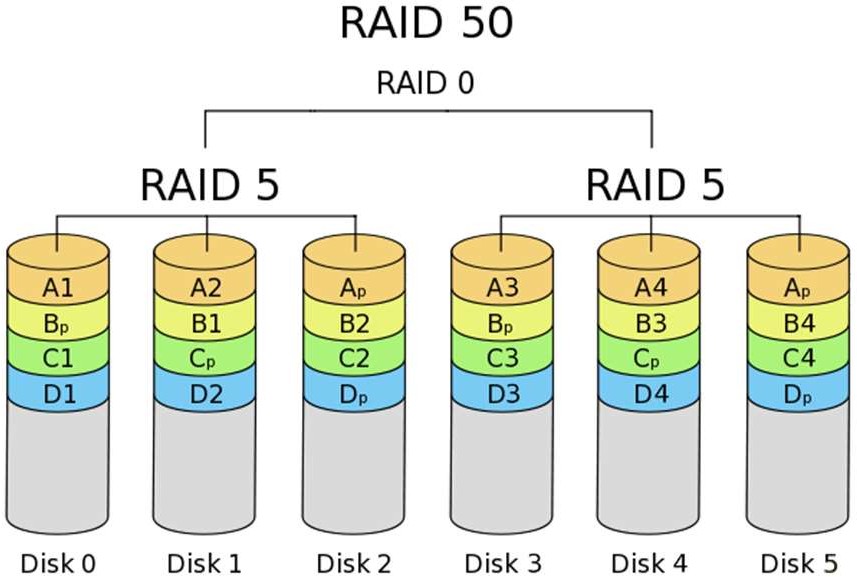
## Комбинирани райд нива

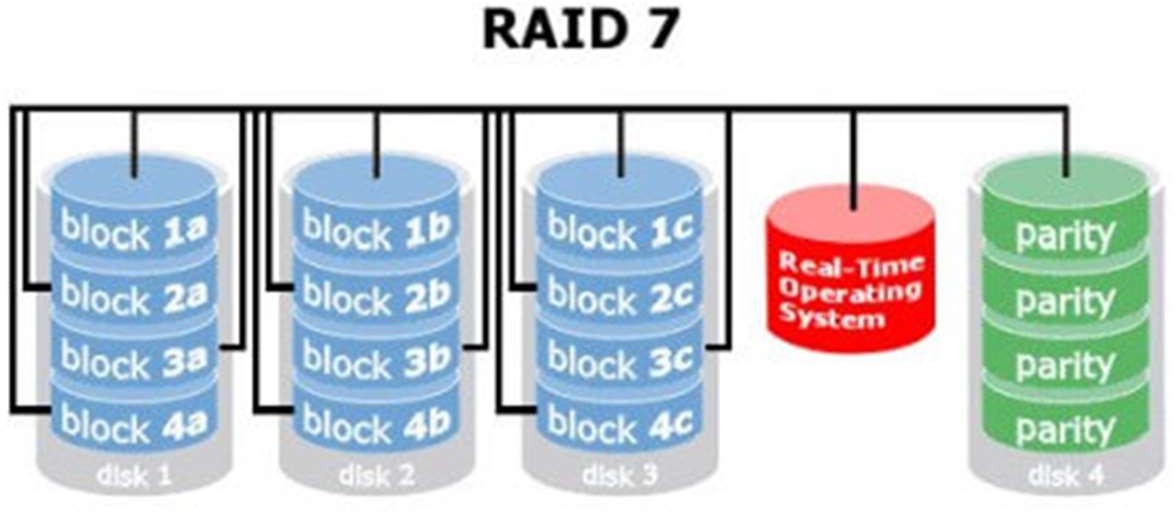
* **RAID 1+0/10** – необходимостта от минимум 4 диска. Това ниво представлява комбинация от RAID 1 и RAID 0. В този случай блоковете от данни се записват огледално (информацията се дублира) и едновременно с това се разпределят между двойка дискове. Тук има по-голяма производителност и защита на данните от RAID 1, но цената му е много по-висока, заради необходимостта от минимум 4 диска. . Масивът може да понесе множество загуби на устройства, стига едно огледално копие да не загуби всичките дискове.
* **RAID 0+1** – отново минималното изискване е 4 дискови устройства. Тук схемата на функциониране е обратна на 1+0. Първо информацията се разпределя последователно на блокове и след това те се дублират. Отново минималното изискване е 4 дискови устройства, което предопределя и високата цена. Рискът от загуба на информация е по-голям, отколкото при RAID 1+0.



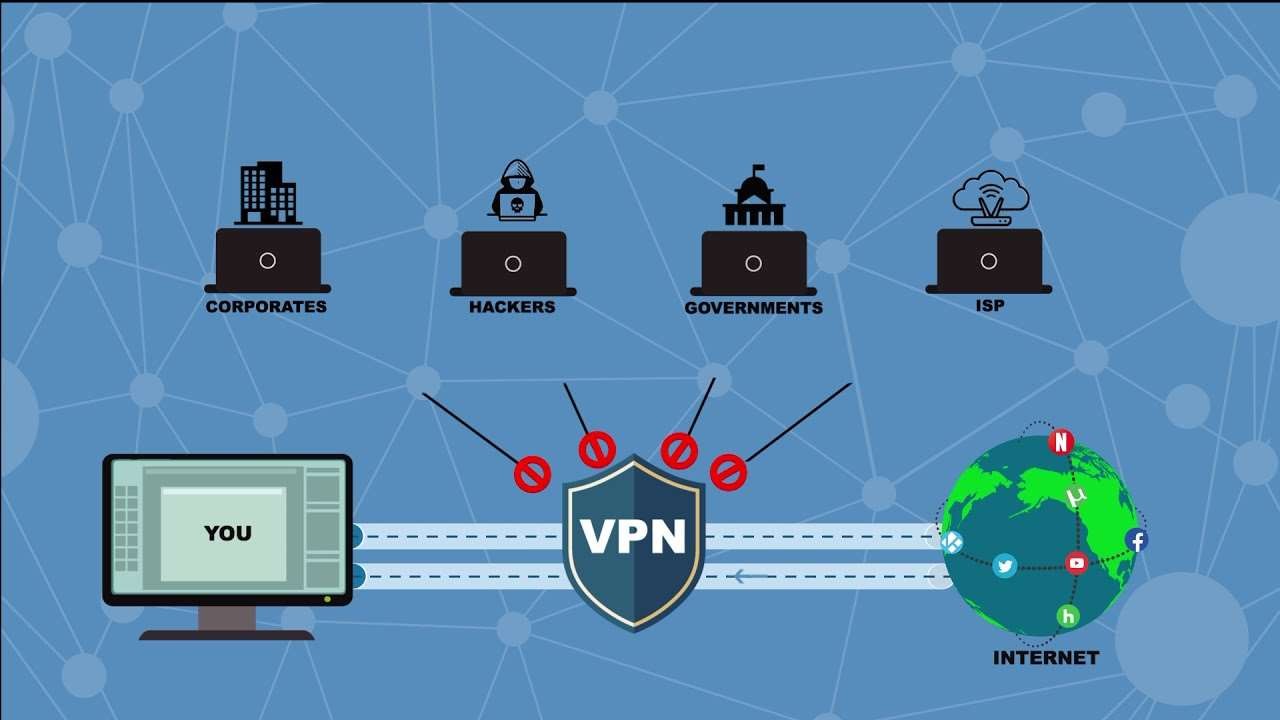
* **RAID 0+3** – нивото обединява начинът на работа на RAID 0 и RAID 3. Използва се разделяне (striping) както при RAID 0, но при разпределение на блоковете по схемата на RAID 3. Така се увеличава надеждността на RAID 3, но с това се повишава и цената.



* **RAID 5+0** – съчетание между разпределението на битовете за четност при RAID 5 със striping-a на RAID 0. Подобрява се надеждността на RAID 5 без да се намалява защитата на данните.
* **RAID 3+4/7** – този RAID е запазена марка на Storage Computer Corporation/за големите корпорации. Показателите на максималния трансфер при четене на файлове, независимо малки или големи, е изключително висок. Начинът на работа обединява RAID 3 и RAID 4, но предлага много по-голяма производителност от тях. Той трудно се намира на пазара и държи висока цена. Най- голямото предимство е максимален трансфер на четене на данните, независимо от размера.



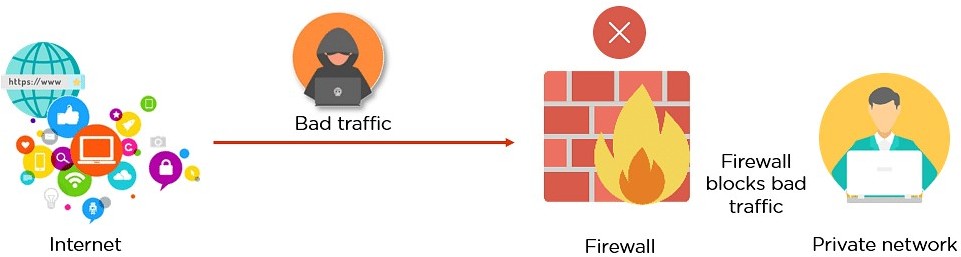
***Приложение 5*** – Хибридни RAID нива



**Фиг. 17** – Функция на VPN-a



**Фиг. 18** – Two-factor authentication

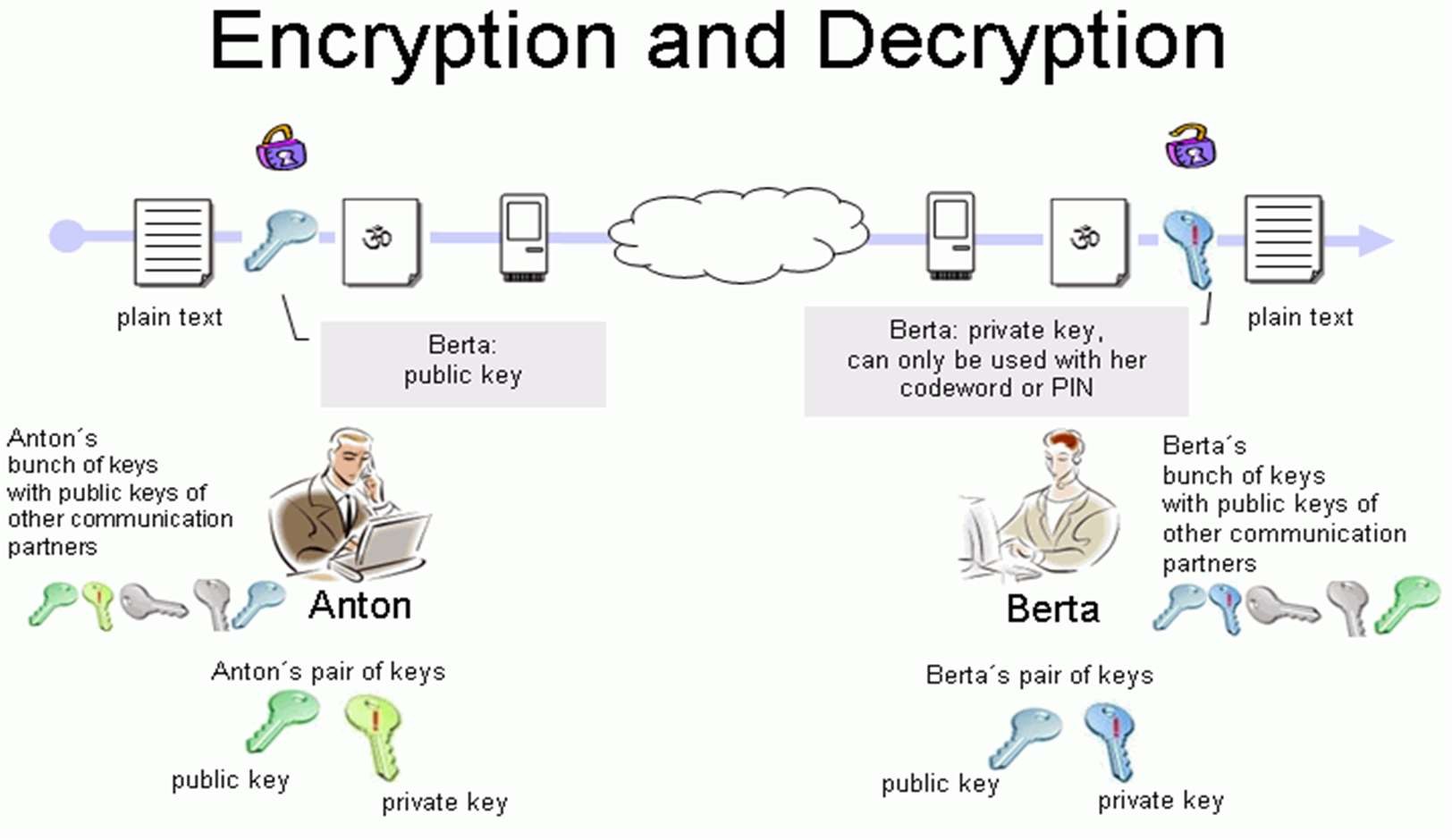


**Фиг. 19** – Функция на Firewall-а



**Фиг. 20** – Функции на антивирусния софтуер

***Препратка 4*** – Уебсайт на Norton – https://ie.norton.com/ps/4up\_norton360\_nav\_ns\_nd\_np\_Reading\_tw\_nb.html?nortoncountry=ie&om\_s em\_cid=hho\_sem\_sy:xs:ggl:en:e:br:kw0000001532:433565143582:c:google:9988471665:9962785429 4:kwd-20964061&gclid=Cj0KCQjwl7qSBhD-ARIsACvV1X2W43urfMtyXRSWO-Mfk7BE- KGoiDB34xLnnIHFYqTo7KrHPZrMu8saAk9aEALw\_wcB&gclsrc=aw.ds



Описание на процеса:

*Антон пише на Берта съобщение.*

*Той криптира съдържанието с публичния ключ на Берта. Берта получава кодирано съобщение.*

*Когато Берта желае да отвори съобщението, нейната програма за електронна поща иска да знае паролата/ПИН кода й.*

*Ако Берта ги въведе правилно, тя може да се прочете съдържанието в обикновен текст.*

**Фиг. 21** – Криптиране и декриптиране

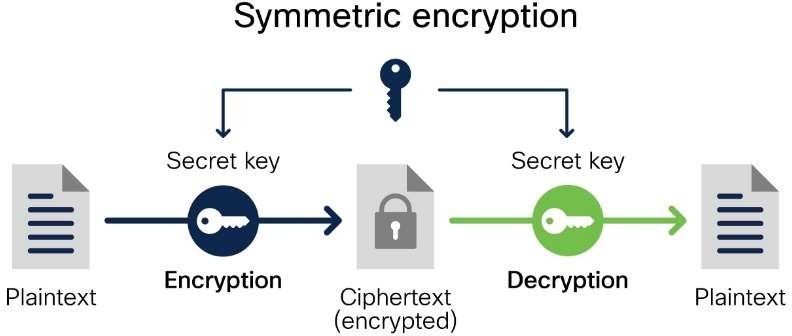
## Пример за SSL

1. Браузърът се свързва със сървъра.
2. Сървърът изпраща своя сертификат към браузъра.

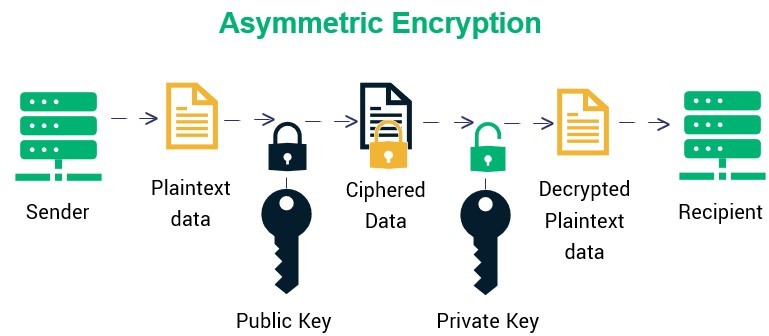
Браузърът прави проверка на сертификата – дали е издаден от валиден сертифициращ орган, дали срокът на валидност на сертификата не е изтекъл, дали името на сайта, което е закодирано в сертификата, отговаря на реалният адрес, който е зареден в браузъра.

1. След като проверките минат успешно браузърът и сървърът определят какъв симетричен криптографски алгоритъм да използват за комуникация, примерно AES, RC4, 3DES и т.н., след което браузърът генерира произволен код (ключ), който криптира с публичния ключ на сървъра и изпраща криптирания код към сървъра.
2. След като сървърът получи кода браузърът вече може да прави заявки към сървъра, като използва за криптиране кода и криптографският алгоритъм, определен със сървъра на предходната стъпка.

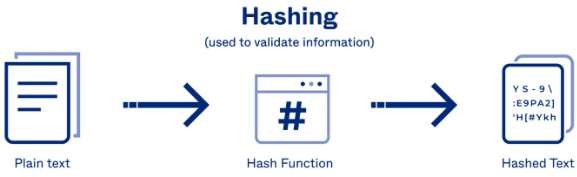
**Фиг. 22** – Пример за SSL



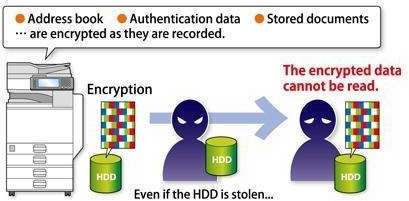
**Фиг. 23** – Симетрично криптиране



**Фиг. 24** – Асиметрично криптиране

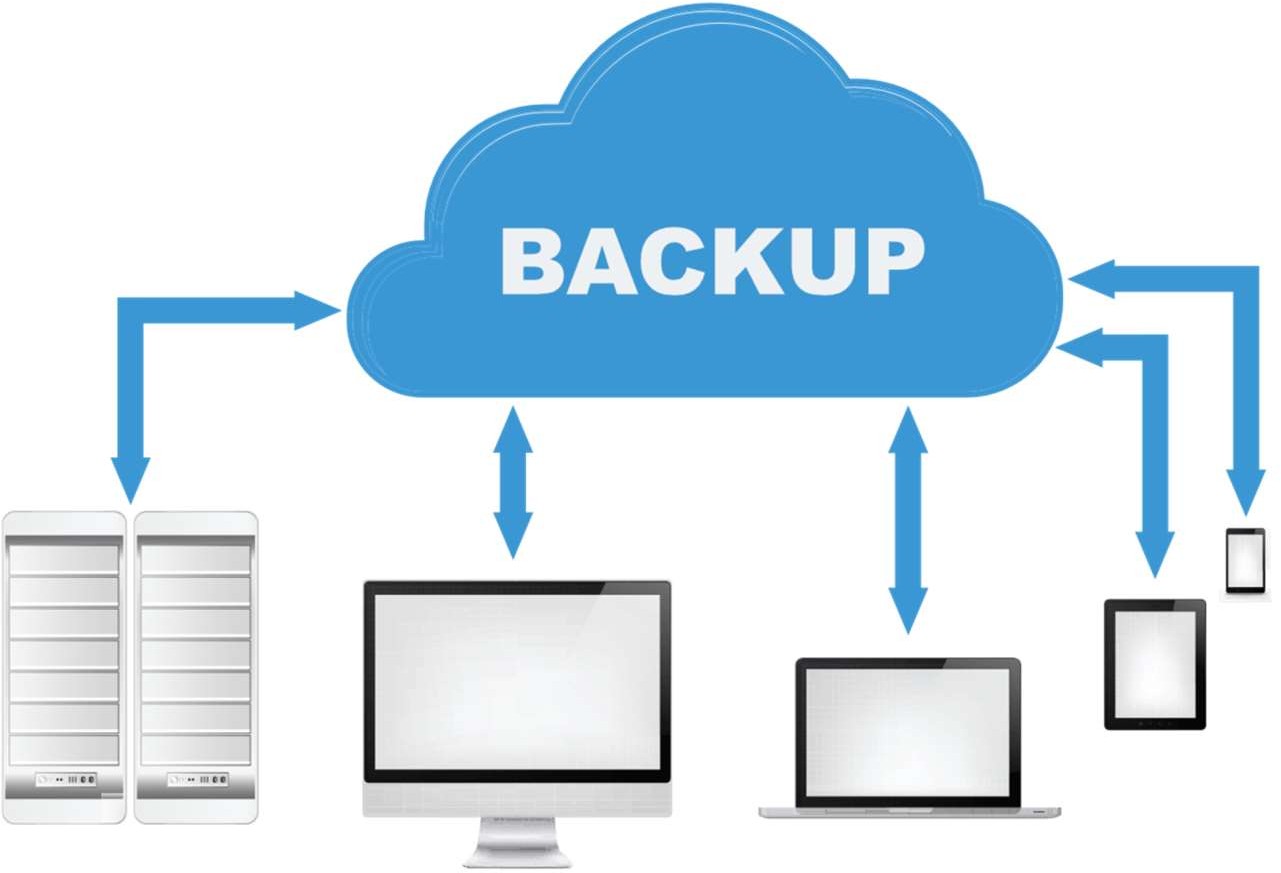


**Фиг. 25** – Хешинг

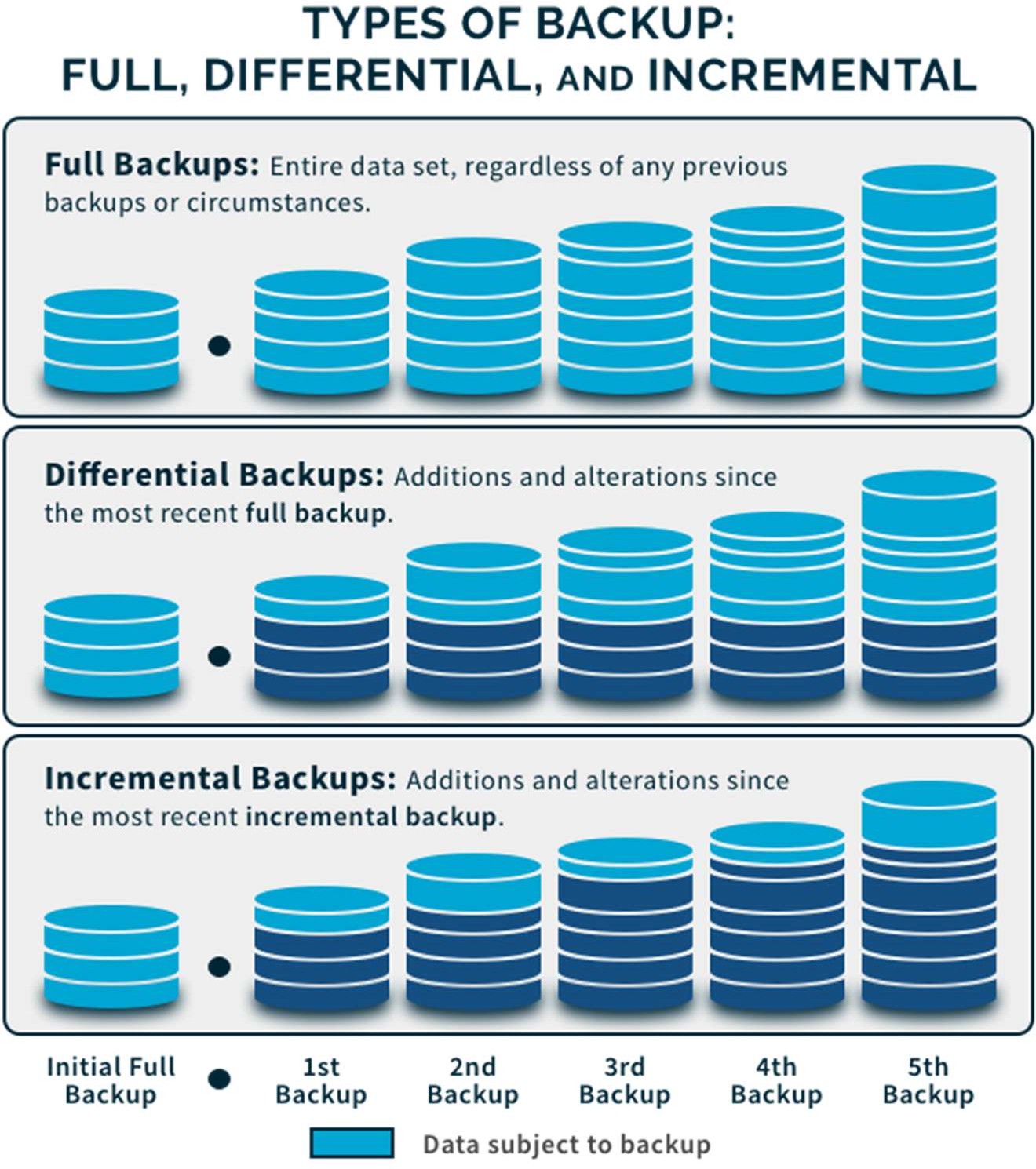


Целият хард диск бива криптиран. След кражба криптираната информация не може да бъде видяна.

**Фиг. 26** – Криптиране на хард диск



**Фиг. 27** – Бекъп



**Фиг. 28** – Full backup, Differential backup, Incremential backup



**Фиг. 29** – Архивиране

|  |  |
| --- | --- |
| Бекъпите са резервно копие на данните, в  случай че стане нещо с тях – бъдат повредени или изтрити. | Архивирането премества данни на друго място, за да освободи пространство. |
| Бекъпите са от решаващо значение за спазването на изискванията, възстановяването при бедствия и  непрекъсваемостта на бизнеса. | Архивите са необходими за постигане на съответствие. |
| Защитава активните и неактивните данни (всички производителни данни). Информацията може да се бекъпне на лента, диск или облак. Резервното копие представлява копие на производствената  информация. |  |
| Обикновено се използва за бързо и мащабно възстановяване. Данните от резервното копие се записват в устройства за дупликация или лентови библиотеки и за по-бърз достъп до големи обеми информация. Приложенията за архивиране могат да се използват за защита на файловете на приложенията и операционната система, в изпълнение към отделните обекти на данни – въпреки че са оптимизирани за възстановявания от по- голям мащаб. Най-добре е за възстановяване на приложения и цели  системи. | Предназначено е за съхраняване на отделни обекти от данни, като имейл съобщения, файлове и бази данни, заедно с техните метаданни. Архивът може да осигури бърз и специфичен достъп до съхраняваната информация – така че лесно да се намери конкретното писмо от преди 5 години. Метаданните могат да помогнат да увеличаване на мащаба на търсенето на съдържание. За разлика от системите за архивиране, архивите не осигуряват възстановяване на ниво обем или на пълен сървър. Те съдържат само подмножество от  данните на бизнеса. |
|  | Поддържането на архивна система за възстановяване при бедствия може да е трудно и скъпо. Организациите често са  принудени да закупят скъпи системи, тъй |

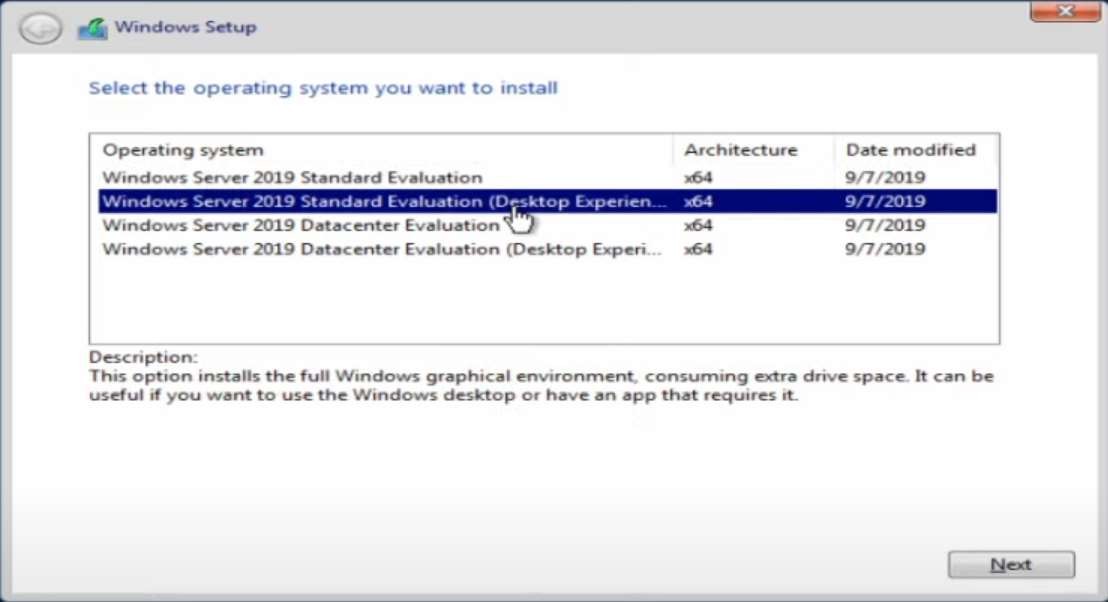
|  |  |
| --- | --- |
|  | като повечето реализации на репликация са патентовани. За разлика от традиционното Disaster recovery, възможността за контрол на репликацията, връщане на данните към предишни точки на възстановяване и управление на използването на честотната лента варира в широки граници, в  зависимост от архивната система. |
|  | Архивите са оптимизирани за евтино и дългосрочно съхранение. Те съхраняват производствени данни, което означава, че загубата или повредата им вероятно ще доведе до постоянна загуба на производствена информация. Тези данни вероятно ще бъдат по-стари или по-малко използвани, но също така може да са  единствено копие. |

Някои организации използват архивираните данни и резервните копия заедно – бекъпването на архива помага да се гарантира неговата цялост. Ако съответствието изисква архиви, организацията трябва да се увери, че се спазват политиките за съхранение, определени от стандартите, за да се избегнат глоби. И архивите, и резервните копия трябва да бъдат адекватно защитени. Неефективната защита на киберсигурността може да направи всички архивирани данни достъпни за кибератаки. Нарушаването на сигурността на данните в архива може да бъде опустошително за целостта на бизнеса и репутацията на марката. Независимо дали става въпрос за бекъпи или архиви, файловете трябва да са плътно защитени от нападатели.

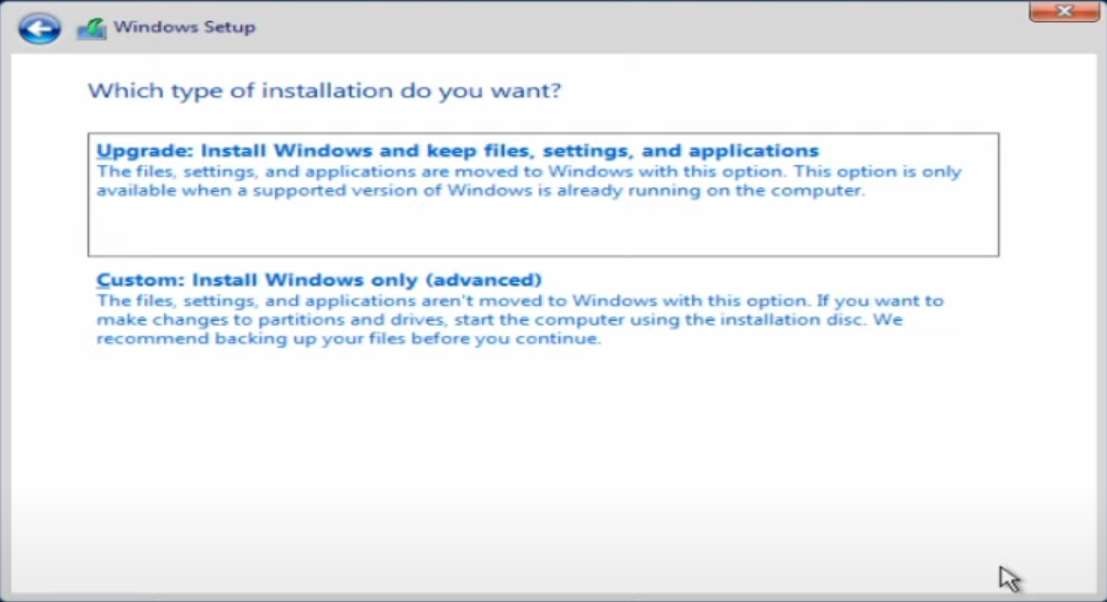
Двете опции могат да бъдат приложени заедно, за да оптимизират цената и да подобрят ефективността на дадена storage инфраструктура. Бекъпа е по-ефективен в среда, която има ефективни решения за архивиране, а и архивите все още превъзхождат бекъп инфраструктурите за техните, заради неговите нужди от защита на данните. И двете решения са важни за ефективна стратегия за управление на данните.

***Таблица 2*** – Съпоставка на бекъп и архивиране

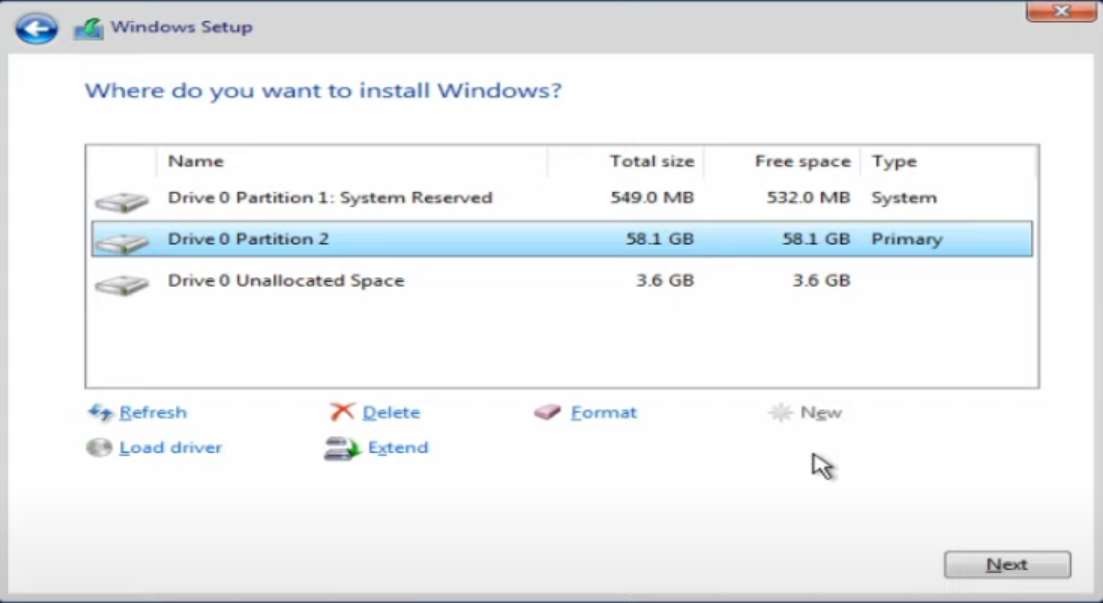
***Препратка 5*** – https://whatisanything.com/what-percentage-of-computer-users-use-windows/ ***Препратка 6*** – https://[www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019](http://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019) ***Препратка 7*** – https://youtu.be/\_3p-f\_Cwa4g



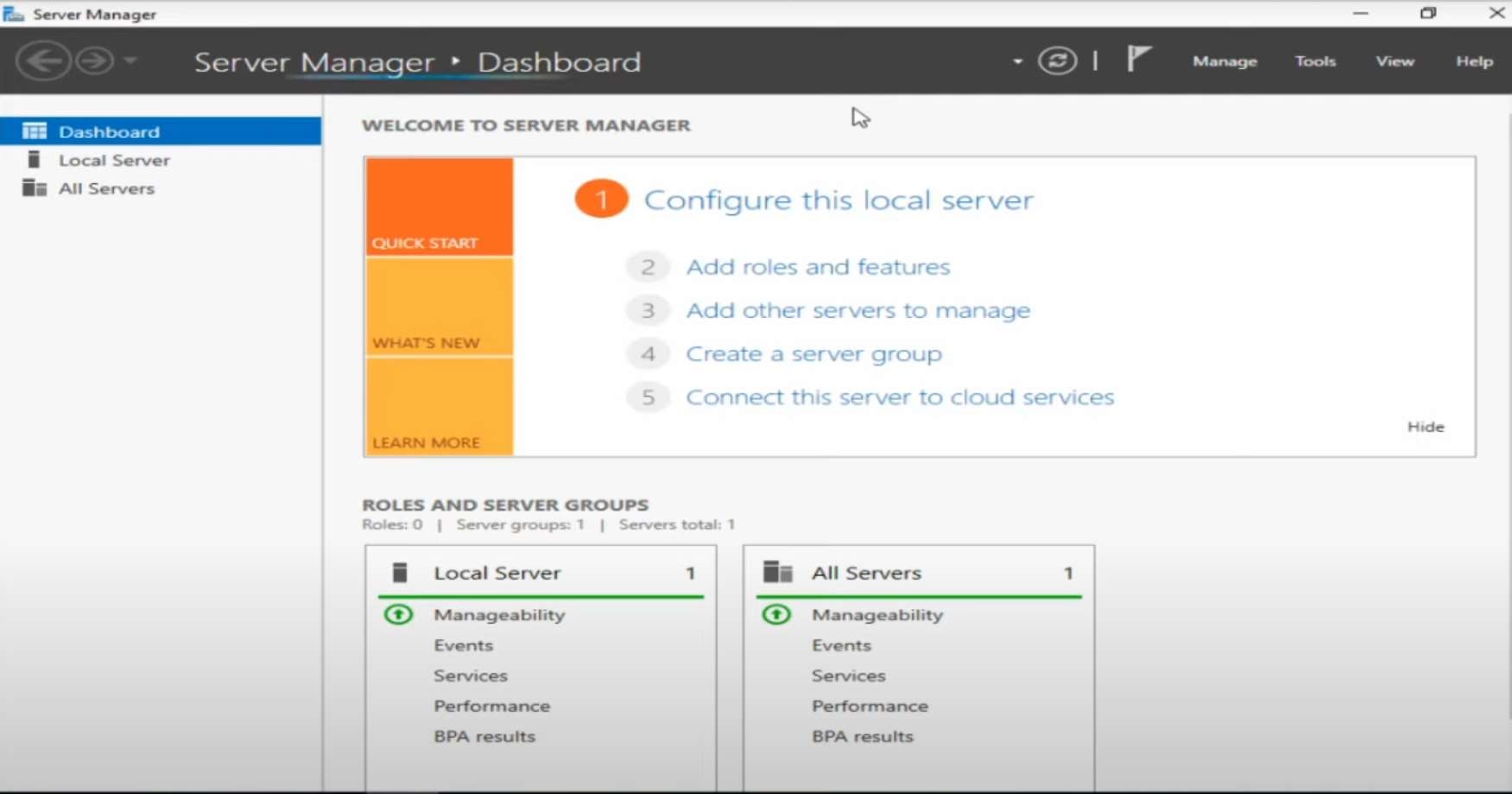
**Фиг. 30** – Селектиране на Windows Server 2019 Standard Evaluation



**Фиг. 31** – Избор между Upgrade или Custom installation

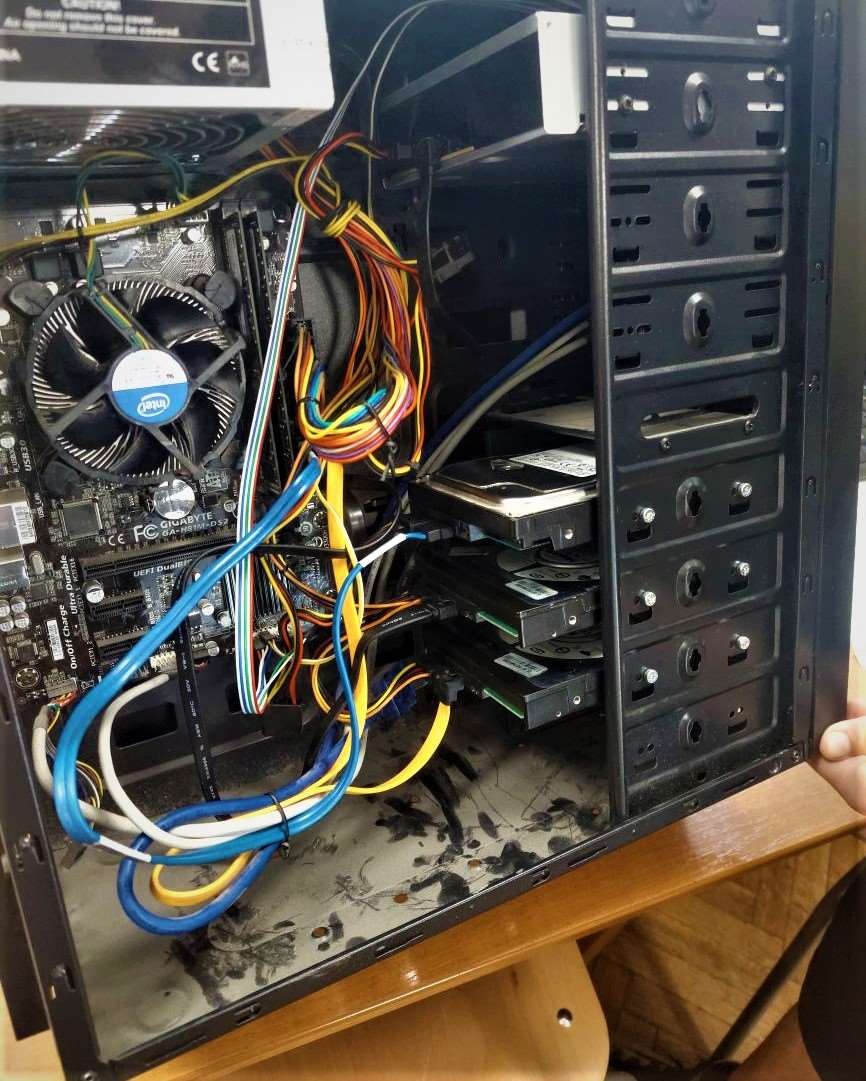


**Фиг. 32** – Делене на партишъни и избиране на коя част от диска ще се намира операционната система

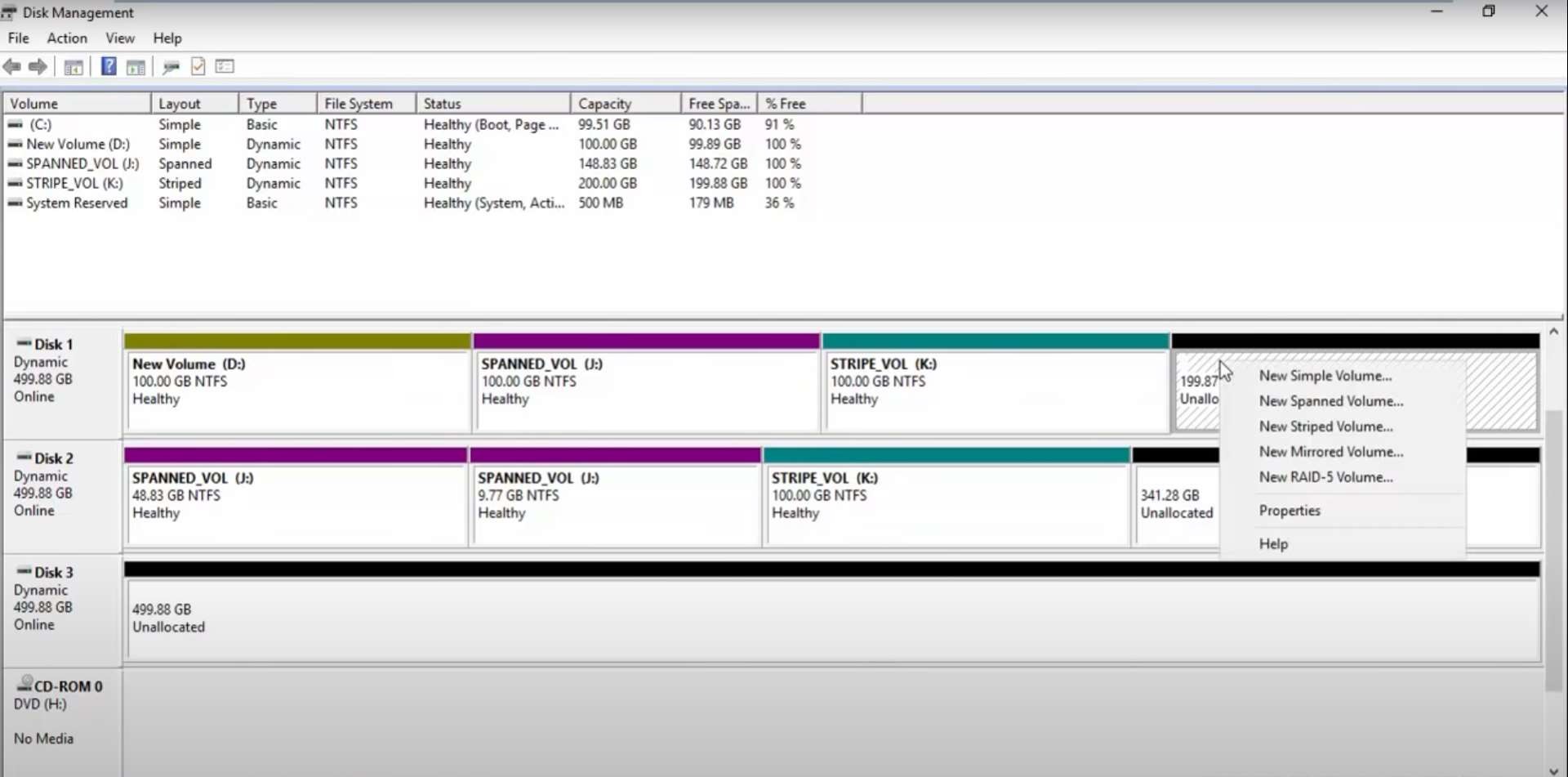


**Фиг. 33** – Server manager

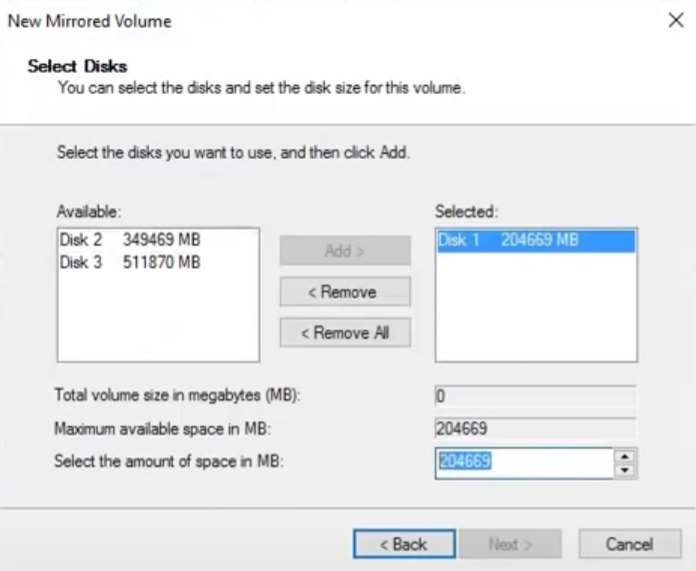
***Препратка 8*** – https://youtu.be/fRBV-NzYAZw



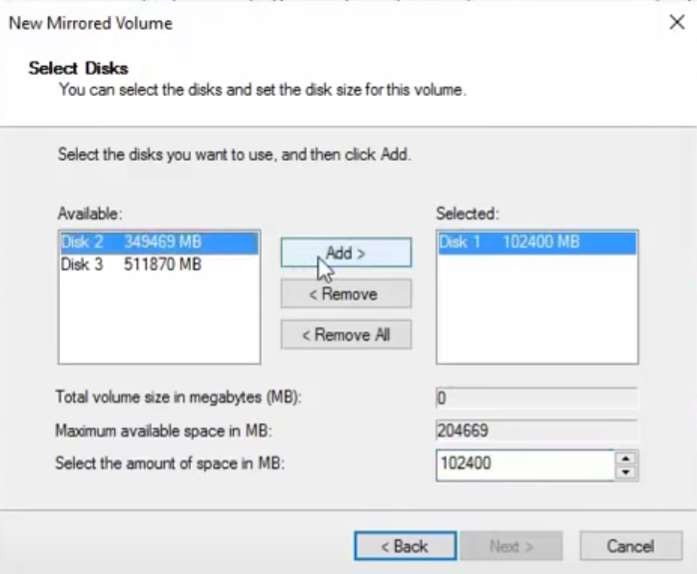
**Фиг. 34** – Двата хард диска по 40 GB (долните, горният е основният хард диск на машината), свързани към машината, посредством SATA кабели.



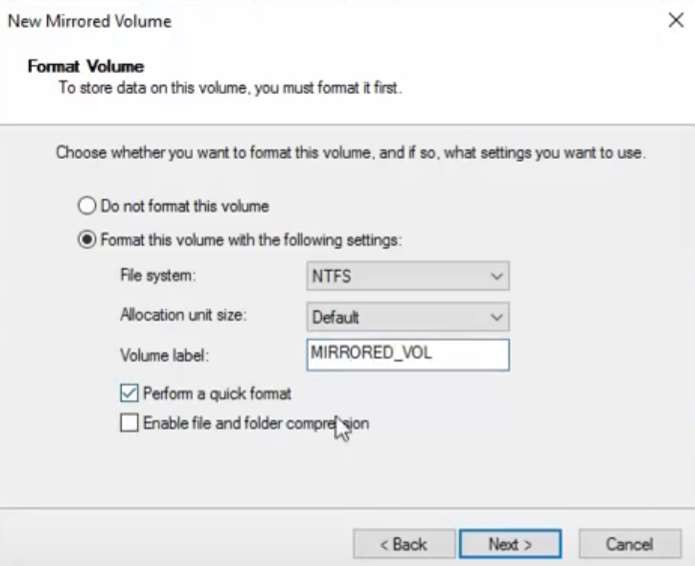
**Фиг. 35** – Десен клавиш върху един от volume-ите



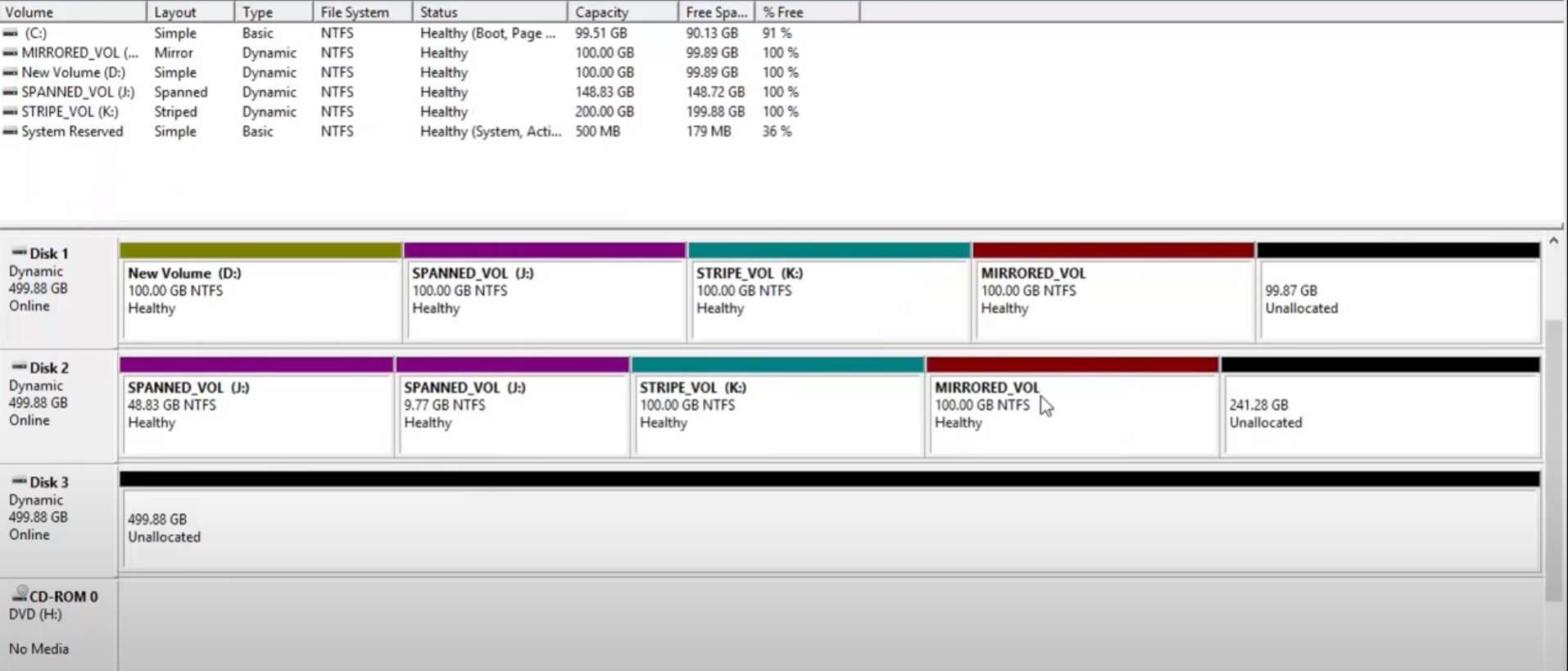
**Фиг. 36** – Определяне на количеството памет, което ще се включи към RAID масива



**Фиг. 37** – Добавяне на втория диск с бутона “Add”



**Фиг. 38** – Задаване на име на новия volume и избирателно селектване на Perform a quick format



**Фиг. 39** – Мирърните дискови простанства ще сменят цвета си в червен



**Фиг. 40** – Избиране на кой от двата диска ще бъде премахнат

***Препратка 9*** – https://youtu.be/SwicvNPg4QU