**ΥΠΟΥΡΓΕΙΟ ΠΟΛΙΤΙΣΜΟΥ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ**
**ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ**

**Κατσούλας Ν., Όροβας Χ., Παναγιωτίδης Σ.**

# ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

## Β' Τάξη ΤΟΜΕΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΕΠΑ.Λ.

## ΣΗΜΕΙΩΣΕΙΣ ΜΑΘΗΤΗ

ΙΝΣΤΙΤΟΥΤΟ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ & ΕΚΔΟΣΕΩΝ
«ΔΙΟΦΑΝΤΟΣ»

ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ
Πρόεδρος: **Γκλαβάς Σωτήριος**

ΓΡΑΦΕΙΟ ΕΡΕΥΝΑΣ, ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ Β΄
Προϊστάμενος: **Μάραντος Παύλος**
Επιστημονικά Υπεύθυνος: **Δρ. Τσαπέλας Θεοδόσιος,** Σύμβουλος Β΄ Πληροφορικής ΙΕΠ

ΣΥΓΓΡΑΦΙΚΗ ΟΜΑΔΑ:
**Κατσούλας Νικόλαος**, Εκπαιδευτικός Πληροφορικής
**Δρ. Όροβας Χρήστος**, Εκπαιδευτικός Πληροφορικής
**Παναγιωτίδης Σωτήρης**, Εκπαιδευτικός Πληροφορικής

ΕΠΙΜΕΛΕΙΑ - ΣΥΝΤΟΝΙΣΜΟΣ ΟΜΑΔΑΣ:
**Κωτσάκης Σταύρος**, Σχολικός σύμβουλος πληροφορικής

ΕΠΙΤΡΟΠΗ ΚΡΙΣΗΣ:
**Αποστολάκης Ιωάννης**, εκπαιδευτικός Πληροφορικής,
**Γώγουλος Γιώργος**, Σχολικός Σύμβουλος Πληροφορικής,
**Μωράκης Διονύσιος**, εκπαιδευτικός Πληροφορικής.

ΦΙΛΟΛΟΓΙΚΗ ΕΠΙΜΕΛΕΙΑ:
**Δελής Φίλιππος,** Εκπαιδευτικός Φιλόλογος

ΠΡΟΕΚΤΥΠΩΤΙΚΕΣ ΕΡΓΑΣΙΕΣ: ΔΙΕΥΘΥΝΣΗ ΕΚΔΟΣΕΩΝ/Ι.Τ.Υ.Ε. «ΔΙΟΦΑΝΤΟΣ»

ΠΕΡΙΕΧΟΜΕΝΑ

# Κεφάλαιο 1

## Βασικές Εισαγωγικές Έννοιες

Ένας υπολογιστής είναι ένα σύνολο από διάφορα τμήματα υλικού (hardware) που συνεργάζονται μεταξύ τους. Μόλις το σύνολο αυτό τροφοδοτηθεί με ηλεκτρικό ρεύμα, τα εξαρτήματα αυτά αρχίζουν να λειτουργούν συντονισμένα. Εμφανίζεται ένα περιβάλλον στο οποίο μπορούμε να εκτελέσουμε διάφορα προγράμματα, από απλά ηλεκτρονικά παιχνίδια μέχρι σύνθετες εφαρμογές επεξεργασίας δεδομένων. Ο συντονιστής αυτών των εξαρτημάτων είναι ένα σύνολο προγραμμάτων που ονομάζεται Λειτουργικό Σύστημα (ΛΣ). Στο κεφάλαιο αυτό παρουσιάζονται τα βασικά στοιχεία του.

**Διδακτικοί Στόχοι**

Σε αυτό το κεφάλαιο θα μάθετε:

- Να περιγράφετε τον ρόλο και την αναγκαιότητα ύπαρξης των Λειτουργικών Συστημάτων (ΛΣ).
- Να αναγνωρίζετε τις διάφορες κατηγορίες των ΛΣ και την εξέλιξη τους.
- Να προσδιορίζετε τα ΛΣ ανοιχτού κώδικα.
- Να εντοπίζετε τις απαιτήσεις των ΛΣ όσον αφορά το υλικό.
- Να αναγνωρίζετε τα ΛΣ φορητών συσκευών.

**Διδακτικές Ενότητες**

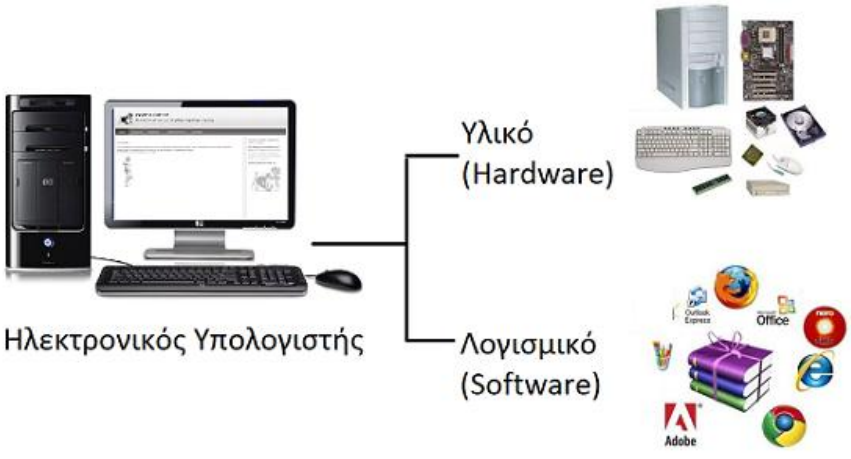
1.1 Λογισμικό Συστήματος
1.2 Τι είναι Λειτουργικό Σύστημα
1.3 Βασικές αρμοδιότητες και λειτουργίες του ΛΣ
1.4 Η δομή ενός λειτουργικού συστήματος
1.5 Ο Πυρήνας (kernel) του λειτουργικού συστήματος
1.6 Η επικοινωνία με τον χρήστη ή Διεπαφή χρήστη (User Interface)
1.7 Κατηγορίες λειτουργικών συστημάτων
1.8 Ιστορική εξέλιξη των ΛΣ

# 1.1. Λογισμικό Συστήματος

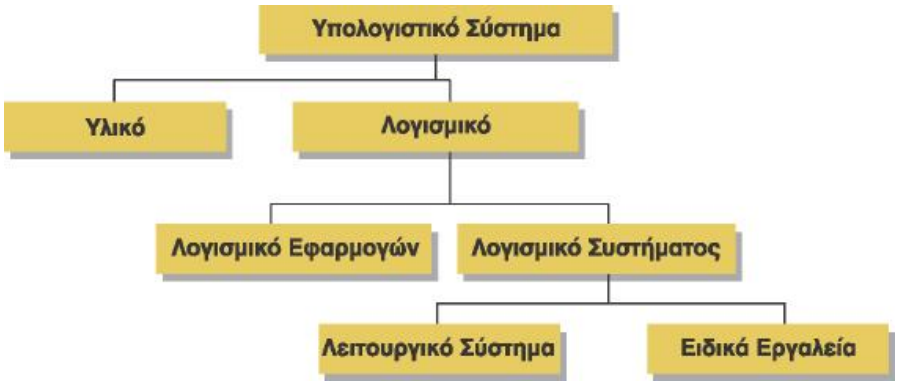
**1.1.1 Οι έννοιες «Πρόγραμμα» και «Λογισμικό»:** Από την στιγμή που θα τροφοδοτηθεί με ηλεκτρικό ρεύμα ο υπολογιστής αρχίζει την εκτέλεση ενός πλήθους προγραμμάτων. Όταν αναφερόμαστε στον όρο **πρόγραμμα** εννοούμε ένα σύνολο εντολών που καθοδηγεί λεπτομερώς έναν υπολογιστή για να εκτελέσει συγκεκριμένες εργασίες. Κάποια από αυτά εκτελούνται αυτόματα και έχουν στόχο τη διαχείριση του υπολογιστή όπως θα δούμε παρακάτω, ενώ κάποια άλλα εκτελούνται μόνο αφού το ζητήσει κάποιος χρήστης.

Η σημαντική διαφοροποίηση του υπολογιστή από άλλες συσκευές επεξεργασίας δεδομένων (π.χ. παιχνιδομηχανές, συστήματα ελέγχου των αυτοκινήτων) είναι η ικανότητα να εκτελεί ένα πλήθος διαφορετικών προγραμμάτων ανάλογα με τις απαιτήσεις και τις ανάγκες του χρήστη. Μια παιχνιδομηχανή μπορεί να εκτελέσει συγκεκριμένα μόνο παιχνίδια μέσω προγραμμάτων που έχουν κατασκευαστεί ειδικά για αυτή ή ο «ηλεκτρονικός εγκέφαλος» ενός σύγχρονου αυτοκινήτου μπορεί να διαχειριστεί ζητήματα ρύθμισης της κατανάλωσης καυσίμων, ελέγχου των αισθητήρων, καταγραφής προβλημάτων λειτουργίας και άλλα ζητήματα ενός συγκεκριμένου μοντέλου ενός συγκριμένου κατασκευαστή αυτοκινήτων. Αντίθετα ο υπολογιστής παρέχει στο χρήστη μια γενική μηχανή με ένα σύνολο στοιχείων υλικού (επεξεργαστής, μνήμη, οθόνη, πληκτρολόγιο, ποντίκι, σκληρός δίσκος και άλλες συσκευές) η οποία μπορεί να προγραμματιστεί να εκτελέσει οποιαδήποτε εφαρμογή επεξεργασίας δεδομένων, από ένα παιχνίδι μέχρι ένα πρόγραμμα ανάλυσης δορυφορικών φωτογραφιών και καιρικών δεδομένων με στόχο τις μετεωρολογικές προβλέψεις.

**Λογισμικό** (software) ονομάζεται το σύνολο των προγραμμάτων που χρησιμοποιούνται στους υπολογιστές. Μαζί με το υλικό (hardware) αποτελούν ένα ολοκληρωμένο υπολογιστικό σύστημα (εικ.1.1).




Εικόνα 1.1: Προσωπικός Υπολογιστής (*πηγή: δικτυογραφία #9*)




Εικόνα 1.2: Υπολογιστής και κατηγορίες λογισμικού *(πηγή: βιβλιογραφία #4*)

Για να γράψει κανείς ένα πρόγραμμα για έναν υπολογιστή, πρέπει να χρησιμοποιήσει κάποια **γλώσσα προγραμματισμού.** Οι γλώσσες προγραμματισμού ανάλογα με τις εντολές που χρησιμοποιούν κατατάσσονται σε διάφορα επίπεδα ανάλογα με το πόσο κοντά βρίσκονται στον άνθρωπο (υψηλού επιπέδου) ή στον υπολογιστή (χαμηλού επιπέδου).

**1.1.2 Είδη Λογισμικού** Όπως φαίνεται και στην εικ. 1.2 το λογισμικό μπορεί να χωρισθεί σε δυο μεγάλες κατηγορίες: Στο λογισμικό εφαρμογών και στο λογισμικό Συστήματος.

**Λογισμικό Εφαρμογών:** Στην κατηγορία αυτή περιλαμβάνεται μια μεγάλη ποικιλία διαφορετικών προγραμμάτων τα οποία είναι κατασκευασμένα για να εκτελούν συγκεκριμένες εργασίες σύμφωνα με τις απαιτήσεις και τις ανάγκες μας. Ανάλογα με τη δραστηριότητα που αναπτύσσουμε επιλέγουμε και το αντίστοιχο πρόγραμμα. Μερικά παραδείγματα λογισμικού εφαρμογών είναι:

- ***Τα προγράμματα σχεδίασης, επεξεργασίας φωτογραφίας, βίντεο, εικόνων, ήχου και πολυμέσων***. Μας παρέχουν τη δυνατότητα να δημιουργήσουμε και να επεξεργαστούμε πληροφορίες αυτού του είδους.
- ***Τα προγράμματα αυτοματισμού γραφείου***. Μπορούμε να γράψουμε και να διαμορφώσουμε ένα κείμενο χρησιμοποιώντας διάφορα είδη γραφής, πίνακες, πλαίσια, εικόνες. Επίσης μπορούμε να χρησιμοποιήσουμε βάσεις δεδομένων και λογιστικά φύλλα.
- ***Τα εκπαιδευτικά προγράμματα***. Μας δίνουν τη δυνατότητα να εκπαιδευτούμε σε κάποιο διδακτικό αντικείμενο (ιστορία, μαθηματικά, φυσικά, χημεία, πληροφορική, και οτιδήποτε γενικά). Επίσης μπορούμε να αναζητήσουμε πληροφορίες σα να είχαμε στη διάθεση μας μια πραγματική εγκυκλοπαίδεια πολλών τόμων.
- **Τα παιχνίδια**. Υπάρχουν πολλές κατηγορίες παιχνιδιών από τα πιο απλοϊκά μέχρι σύνθετα παιχνίδια στρατηγικής και δράσης.
- **Οι φυλλομετρητές**. Μας επιτρέπουν να κάνουμε περιήγηση στο διαδίκτυο και να χρησιμοποιούμε δικτυακές εφαρμογές.

**Λογισμικό Συστήματος:** Στην κατηγορία αυτή περιλαμβάνονται όλα τα προγράμματα που χρησιμοποιούνται για τον έλεγχο της λειτουργίας του υπολογιστή και τη δημιουργία και εκτέλεση των προγραμμάτων εφαρμογών. Το βασικότερο λογισμικό της κατηγορίας αυτής είναι το **Λειτουργικό Σύστημα (ΛΣ, Operating System, OS).** Το ΛΣ είναι ένα σύνολο προγραμμάτων που είναι υπεύθυνα για τη σωστή και συντονισμένη λειτουργία του υπολογιστή και τη διαθεσιμότητα των δυνατοτήτων του σε άλλα προγράμματα ή στον χρήστη. Στη κατηγορία του

λογισμικού συστήματος ανήκουν επίσης και τα **ειδικά εργαλεία** (**utilities**) όπως προγράμματα ελέγχου και διαμόρφωσης του σκληρού δίσκου, ελέγχου και επιδιόρθωσης δυσλειτουργιών του υπολογιστή, ανάλυσης της κίνησης δεδομένων σε ένα δίκτυο υπολογιστών κ.ά.


Εικόνα 1.3: Τα εμπορικά σήματα που αντιπροσωπεύουν κάποια λειτουργικά συστήματα.

## 1.2. Τι είναι Λειτουργικό Σύστημα

Όπως αναφέρθηκε, το ΛΣ αποτελείται από μία ομάδα προγραμμάτων τα οποία ενεργούν ως "ενδιάμεσο" μεταξύ του υπολογιστή και των χρηστών, εφαρμογών και περιφερειακών που κάνουν χρήση του.


Εικόνα 1.4: Το ΛΣ προσομοιάζεται με τον μαέστρο του υπολογιστή *(πηγή: βιβλιογραφία #2*)

Το Λειτουργικό Σύστημα επιτρέπει στον υπολογιστή να αντιλαμβάνεται τις οδηγίες που του δίνουμε μέσω των συσκευών εισόδου (πληκτρολόγιο, ποντίκι κ.ά). Μας επιτρέπει επίσης να επικοινωνούμε με τα προγράμματα δια μέσου της οθόνης του υπολογιστή, να αποθηκεύουμε στοιχεία σε δίσκους και flash disks και γενικά να επικοινωνούμε και να διαχειριζόμαστε τις περιφερειακές συσκευές.

Γενικά ένα Λειτουργικό Σύστημα είναι υπεύθυνο για την αρμονική λειτουργία και διαχείριση του υλικού του υπολογιστή, την επικοινωνία μας με αυτόν και την εκτέλεση άλλων προγραμμάτων.

Με την ανάπτυξη της τεχνολογίας και την εμφάνιση των σύγχρονων «έξυπνων» κινητών τηλεφώνων ο ρόλος του λειτουργικού συστήματος έγινε πιο κατανοητός. Όλες οι συσκευές αυτού του τύπου, ανεξαρτήτως κατασκευαστή, διαχειρίζονται πλέον μέσω ενός κοινώς γνωστού περιβάλλοντος (π.χ Android) το οποίο επιτρέπει την εκτέλεση εφαρμογών για πραγματοποίηση κλήσεων, περιήγηση στο διαδίκτυο, λήψη φωτογραφιών κτλ

Η εικόνα 1.4 παρομοιάζει πολύ επιτυχημένα ένα Λειτουργικό Σύστημα (ή το ρόλο ενός λειτουργικού συστήματος) με το μαέστρο μιας ορχήστρας. Οι μουσικοί με τα μουσικά όργανα είναι τα μέρη του υλικού ενώ οι παρτιτούρες της μουσικής με τις νότες είναι τα προγράμματα. Σε αυτό το παράδειγμα ο χρήστης έχει τον ρόλο του κοινού που απολαμβάνει το τελικό αποτέλεσμα.

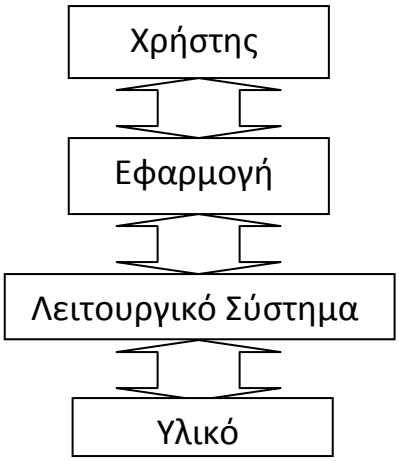
## 1.3. Βασικές αρμοδιότητες και λειτουργίες του Λειτουργικού Συστήματος

Οι βασικές "αρμοδιότητες" του λειτουργικού συστήματος είναι λοιπόν:

- Να λειτουργεί ως ενδιάμεσος (Διεπαφή ή Interface) ανάμεσα στον άνθρωπο και στη μηχανή.
- Να διαχειρίζεται τις δυνατότητες και τους πόρους (resources) του συστήματος υπολογιστή έτσι, ώστε να παράγεται χρήσιμο έργο.
- Να μεταφέρει εντολές ή/και απαιτήσεις του χρήστη στον Η/Υ.
- Να δίνει χρήσιμες πληροφορίες για την κατάσταση του συστήματος, μεταφέρει μηνύματα του Η/Υ προς το χρήστη για λάθη ή προβλήματα που εμφανίζονται.
- Να διαχειρίζεται την Κεντρική Μνήμη (RAM) του συστήματος.
- Να ενεργοποιεί και δίνει οδηγίες στην ΚΜΕ. κατανέμοντας το χρόνο λειτουργίας της στους χρήστες και στα διάφορα προγράμματα που εκτελούνται.
- Να διαχειρίζεται τις συσκευές εισόδου και εξόδου ελέγχοντας τη ροή των δεδομένων (είσοδος) και την έξοδο των πληροφοριών (έξοδος).
- Να οργανώνει και διαχειρίζεται τα αρχεία του συστήματος μέσω του συστήματος αρχείων.
- Να ελέγχει την εκτέλεση των προγραμμάτων των χρηστών.
- Να εφαρμόζει μηχανισμούς που βελτιώνουν την ασφάλεια του υπολογιστή από διάφορους κινδύνους.

Ενα ΛΣ έχει δυο βασικούς σκοπούς:

Ο *πρώτος* βασικός σκοπός ενός λειτουργικού συστήματος είναι η διευκόλυνση του χρήστη στην επικοινωνία του με τον υπολογιστή. Η διευκόλυνση αυτή επιτυγχάνεται με τη δημιουργία ενός




Εικόνα 1.5 Επίπεδα ενός συστήματος υπολογιστή

περιβάλλοντος επικοινωνίας (φλοιού). Αυτό μεσολαβεί ανάμεσα στο χρήστη και τον υπολογιστή και έτσι δεν είναι απαραίτητο ο χρήστης να γνωρίζει λεπτομέρειες του υλικού για να κάνει χρήση του.

Ο χρήστης λοιπόν μπορεί να εστιάσει σε αυτό που επιθυμεί να γίνει και με τις εντολές του και τα προγράμματα εφαρμογών που χρησιμοποιεί να λύσει ένα πρόβλημά του. Το ΛΣ είναι στη συνέχεια υπεύθυνο για την μεταβίβαση στο υλικό των ενεργειών που πρέπει να γίνουν.

Για παράδειγμα, ο χρήστης δίνει μια εντολή για την αντιγραφή ενός αρχείου από το σκληρό δίσκο σε ένα flash disk. Το ΛΣ αναγνωρίζει την εντολή του χρήστη, αναζητά το αρχείο στο δίσκο, εντοπίζει τη θέση του, ελέγχει αν υπάρχει ελεύθερος χώρος στο flash disk και αρχίζει τη μεταφορά του αρχείου ενότητά - ενότητα από το ένα μέσο στο άλλο.

Ο *δεύτερος* σκοπός ενός λειτουργικού συστήματος είναι η αξιόπιστη και η αποδοτική λειτουργία του συστήματος του υπολογιστή και η καλύτερη αξιοποίηση των πόρων του (ΚΜΕ, μνήμη, δίσκοι, περιφερειακές συσκευές). Όπως θα δούμε και στα επόμενα κεφάλαια, η κατανομή αυτών των πόρων γίνεται με βάση κριτήρια τα οποία εξασφαλίζουν ίση χρήση από όλους τους ενδιαφερόμενους (χρήστες και εφαρμογές) και αποτελεσματικότητα στην αξιοποίηση τους.

## 1.4. Η δομή ενός λειτουργικού συστήματος

Ένα ΛΣ αποτελείται από τα παρακάτω τμήματα:

**α) Τον Πυρήνα (Kernel).** Είναι το κυριότερο τμήμα ενός ΛΣ. Το τμήμα αυτό φορτώνεται πρώτο στην κύρια μνήμη και εκτελείται συνεχώς σε όλη τη διάρκεια λειτουργίας του υπολογιστή. Τα προγράμματα εφαρμογών επικοινωνούν με αυτό μέσα από ένα καθορισμένο σύνολο κλήσεων. Ο πυρήνας είναι ο κύριος υπεύθυνος για τη συνεργασία του λογισμικού με το υλικό του υπολογιστή,

**β) Το Σύστημα Αρχείων (File System).** Είναι το τμήμα του ΛΣ το οποίο διαχειρίζεται τα αρχεία (ονοματοδοσία, καταχώριση, ανάκτηση κ.λπ.) και φροντίζει επίσης για τη διάθεσή τους στους χρήστες,

**γ) Τη διεπαφή χρήστη (user interface).** Είναι το τμήμα που αναλαμβάνει να δέχεται και να δίνει στο σύστημα του υπολογιστή τα αιτήματα (εντολές) του χρήστη και επίσης να μεταφέρει στο χρήστη μηνύματα από το σύστημα. Το τμήμα αυτό δημιουργεί το περιβάλλον επικοινωνίας

χρήστη – υπολογιστή και μπορεί να υλοποιηθεί με *περιβάλλον γραμμής εντολών* ή με *γραφικό περιβάλλον* ή και με τους δύο τρόπους.

## 1.5. Πυρήνας (Kernel) του λειτουργικού συστήματος

Ο Πυρήνας του λειτουργικού συστήματος είναι ένα σύνθετο πρόγραμμα το οποίο διαχειρίζεται αιτήματα χρήσης συσκευών εισόδου/εξόδου από τις εφαρμογές και ελέγχει την κατανομή της μνήμης και της κεντρικής μονάδας επεξεργασίας (ΚΜΕ) στα προγράμματα που εκτελούνται. Αποτελεί το πιο χαμηλό (κοντά στη μηχανή) επίπεδο του ΛΣ και είναι το πρόγραμμα που εκκινεί άμεσα με το άνοιγμα του υπολογιστή και τερματίζει τελευταίο.

Ο πυρήνας χειρίζεται αυτό που ονομάζεται κλήσεις συστήματος. Αυτές είναι αιτήματα από τις εφαρμογές για χρήση του υλικού, δημιουργία νέων διεργασιών που θα εκτελούνται στην ΚΜΕ και διαχείριση της μνήμης του συστήματος. Η επικοινωνία με το υλικό (άλλα και με τις εφαρμογές) πραγματοποιείται δια μέσου ενός συστήματος **διακοπών** που είναι ένας βασικός μηχανισμός του ΛΣ. Μόλις δημιουργείται μια διακοπή που αντιστοιχεί σε κάποιο αίτημα καλείται το αντίστοιχο πρόγραμμα για να διαχειριστεί το αίτημα αυτό. Περισσότερα όμως για αυτές τις λειτουργίες θα δούμε στο 3$^{ο}$ κεφάλαιο.

## 1.6. Η επικοινωνία του χρήστη ή Διεπαφή χρήστη (User Interface)

Αναφέρθηκε προηγουμένως ότι ο πρώτος βασικός σκοπός του ΛΣ είναι η διευκόλυνση του χρήστη στην επικοινωνία με τον υπολογιστή. Αυτός ο ρόλος καλύπτεται από τη λεγόμενη **διεπαφή χρήστη** (user interface) η οποία είναι ένας μηχανισμός που επιτρέπει στον χρήστη: (1) να χρησιμοποιεί αποδοτικά το σύστημα αρχείων, (2) να εκκινεί και να διαχειρίζεται τις εφαρμογές που εκτελούνται στον υπολογιστή και (3) να έχει πληροφορίες για τη λειτουργία των μονάδων του υπολογιστή με δυνατότητα να προβεί σε ρυθμίσεις.

Η διεπαφή χρήστη μπορεί να πραγματοποιηθεί με δύο κυρίως τρόπους:

- Μέσω ενός διερμηνευτή εντολών.
- Μέσω ενός γραφικού περιβάλλοντος επικοινωνίας.

**1.6.1 Διερμηνευτής εντολών.** Ο διερμηνευτής εντολών είναι ο πρώτος ιστορικά μηχανισμός επικοινωνίας με τον υπολογιστή. Ο χρήστης χρησιμοποιεί ένα προκαθορισμένο σύνολο εντολών τις οποίες μπορεί να δώσει στον υπολογιστή δια μέσου μιας τερματικής συσκευής χαρακτήρων (ή ενός αναγνώστη καρτών στις πολύ παλιές εποχές..). Αυτές οι εντολές μπορούν να παραμετροποιηθούν ως προς τη λειτουργία τους. Επίσης, ανάλογα με το ΛΣ, παρέχεται η δυνατότητα συγγραφής σεναρίων. Σε αυτή την περίπτωση μπορεί να αυτοματοποιηθούν πολλές εργασίες που απαιτούν τη χρήση πολλών από αυτές τις εντολές. Λόγω των πολύ ισχυρών δυνατοτήτων και της οικονομίας χρόνου που μπορούμε να έχουμε με τη χρήση αυτών των εντολών, η χρήση του διερμηνευτή εντολών συνεχίζει να υπάρχει ακόμα και στα σύγχρονα λειτουργικά συστήματα. Αυτό γίνεται με τη χρήση ενός ειδικού προγράμματος εξομοίωσης τερματικού.

***Microsoft Windows [Έκδοση 6.1.7601]***
***Πνευματικά δικαιώματα (c) 2009 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματος.***

***C:\Users\osnotes>help***
***Για περισσότερες πληροφορίες σχετικά με μια συγκεκριμένη εντολή, πληκτρολογήστε HELP όνομα-εντολής.***
***ASSOC*** ***Εμφανίζει ή τροποποιεί συσχετίσεις επέκτασης αρχείων.***
***ATTRIB*** ***Εμφανίζει ή αλλάζει τα χαρακτηριστικά αρχείων.***
***BREAK*** ***Ορίζει ή απαλείφει τον εκτεταμένο έλεγχο CTRL+C.***
***BCDEDIT*** ***Καθορίζει ιδιότητες στη βάση δεδομένων εκκίνησης για τον έλεγχο φόρτωσης εκκίνησης.***
***CACLS*** ***Εμφανίζει ή τροποποιεί λίστες ελέγχου πρόσβασης (ACL) αρχείων.***
***CALL*** ***Καλεί ένα πρόγραμμα δέσμης από ένα άλλο.***
***CD*** ***Εμφανίζει το όνομα ή τις αλλαγές του τρέχοντος καταλόγου.***

Εικόνα 1.6: Τμήμα της εξόδου της εντολής HELP η οποία δίνεται μέσω του προγράμματος προσομοίωσης τερματικού cmd.exe στα Windows 7

Παρά το ότι ένας διερμηνευτής εντολών μας δίνει πολλές δυνατότητες μαζικής κυρίως επεξεργασίας αρχείων, εντούτοις είναι δύσκολη η χρήση του, διότι απαιτεί εξοικείωση με τις εντολές και τις παραμέτρους του. Αποτελεί σημαντικό εργαλείο για διαχειριστές συστημάτων και πεπειραμένους χρήστες και μπορεί να εξοικονομήσει χρόνο και να αυτοματοποιήσει διαδικασίες. Στα δε συστήματα UNIX ή στα βασιζόμενα σε αυτό (π.χ LINUX) υπάρχουν περισσότεροι του ενός διερμηνευτές εντολών με πολύ προχωρημένες δυνατότητες προγραμματισμού (sh, csh, bash).

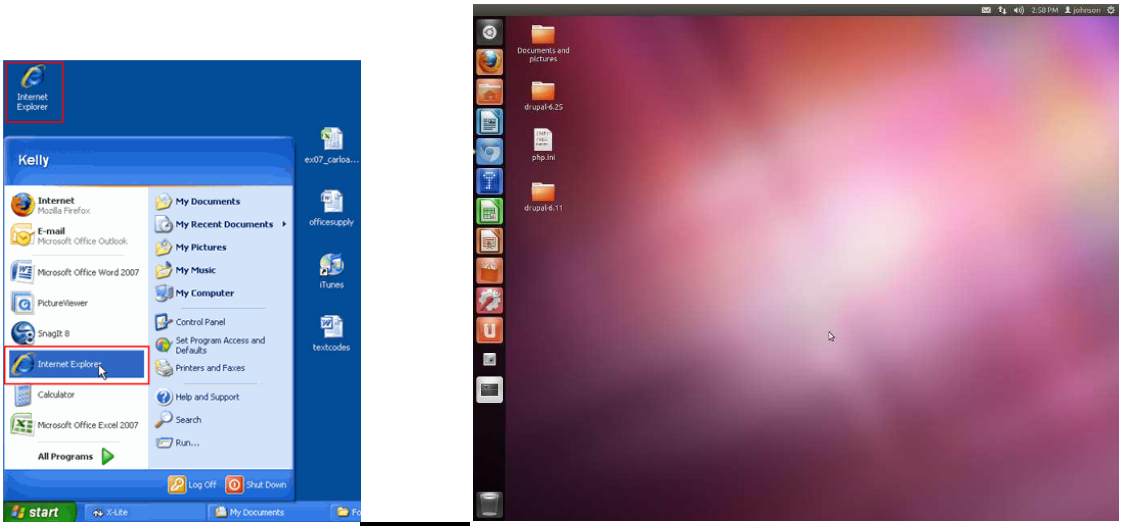
### 1.6.2 Γραφικό περιβάλλον επικοινωνίας

Το γραφικό περιβάλλον επικοινωνίας (Graphical User Interface, GUI) εμφανίζεται από τα μέσα της δεκαετίας του 80 και έπειτα και έχει γίνει πλέον ο βασικός μηχανισμός επικοινωνίας με τον υπολογιστή. Βασικά στοιχεία του είναι τα εξής:

- Η χρήση περιβάλλοντος γραφικών και όχι απλής γραμμής κειμένου.
- Η χρήση «παραθύρων» που είναι ορθογώνιες περιοχές στην οθόνη εντός των οποίων μπορούν να εκτελούνται εφαρμογές. Τα παράθυρα αυτά έχουν έναν καθορισμένο τρόπο εμφάνισης και χειρισμού (τίτλος παραθύρου, χρώματα πλαισίου, μεγιστοποίηση, ελαχιστοποίηση, κλείσιμο).
- Ύπαρξη μιας «επιφάνειας εργασίας» στην οποία μπορούν να υπάρχουν τα παράθυρα των εκτελούμενων εφαρμογών καθώς και εικονίδια που αντιστοιχούν σε εφαρμογές, αρχεία και φακέλους.
- Πλήρης έλεγχος μέσω συσκευών κατάδειξης (π.χ ποντίκι, light pen, touch pad, οθόνη αφής). Ο χρήστης μπορεί να εκκινήσει και να τερματίσει εφαρμογές, να αλλάξει θέση και μέγεθος στα παράθυρα και γενικά να προκαλεί «γεγονότα» (π.χ πάτημα πλήκτρου ποντικιού, τοποθέτηση δείκτη ποντικιού σε μια περιοχή, κ.ά) τα οποία διαχειρίζονται από το ΛΣ και οδηγούνται προς τις αντίστοιχες εφαρμογές για έλεγχο και ανταπόκριση.

- Δυνατότητα ύπαρξης μιας περιοχής όπου υπάρχει ένα «μενού» των εφαρμογών.
- Δυνατότητα ύπαρξης μιας περιοχής όπου εμφανίζονται (σε μορφή εικονιδίων) οι εφαρμογές που εκτελούνται και διάφορες άλλες πληροφορίες (π.χ ώρα)

Για τη χρήση όλων αυτών των δυνατοτήτων από τις εφαρμογές το ΛΣ παρέχει μια σειρά κλήσεων οι οποίες είναι διαθέσιμες δια μέσου βιβλιοθηκών λογισμικού. Το γραφικό περιβάλλον επικοινωνίας μπορεί να είναι αναπόσπαστο κομμάτι του ΛΣ (π.χ όπως συμβαίνει σε όλα τα Microsoft Windows) ή να επιλέγεται/εγκαθίσταται από τον χρήστη (π.χ λειτουργικά Linux με δυνατότητα χρήσης του KDE, του Gnome, κ.ά).




Εικόνα1.7: Παραδείγματα γραφικού περιβάλλοντος (Windows XP (στα αριστερά) και Ubuntu στα δεξιά)

## 1.7. Κατηγορίες λειτουργικών συστημάτων

Σε μια προσπάθεια κατηγοριοποίησης των λειτουργικών συστημάτων θα μπορούσαμε να κάνουμε διακρίσεις ανάλογα με τα παρακάτω:

- Τύπο της επεξεργασίας πληροφοριών που υποστηρίζουν
- Υποστήριξη ενός ή πολλών χρηστών
- Ανοικτό η κλειστό λογισμικό

Εννοείται ότι ένα Λειτουργικό μπορεί να κατατάσσεται ταυτόχρονα σε διάφορες κατηγορίες ανάλογα με τα συγκεκριμένα γνωρίσματα του.

**1.7.1 Κατάταξη με τύπο επεξεργασίας πληροφοριών.** Ανάλογα με τον τύπο επεξεργασίας διακρίνουμε τις κατηγορίες που θα αναφερθούν παρακάτω και οι οποίες διαφοροποιούνται βασικά στο χρόνο απόκρισης και στη γεωγραφική διασπορά των μονάδων. Θα πρέπει να τονιστεί εδώ ότι αυτή η κατηγοριοποίηση συμπεριλαμβάνει κάποιους τύπους λειτουργικών οι οποίοι ουσιαστικά δεν υφίστανται πλέον λόγω της τεράστιας εξέλιξης της τεχνολογίας και της

αύξησης της υπολογιστικής ισχύος, της μνήμης, του αποθηκευτικού χώρου και της ταχύτητας της δικτυακής επικοινωνίας.

- *Κατά δέσμες (batch).* Αν και συναντάται σε παλαιότερα συστήματα, υπάρχουν και σήμερα κατά κάποιο τρόπο στα συστήματα GRID (υπολογιστικά πλέγματα). Πάρα πολλοί χρήστες αναθέτουν τις συνήθως απαιτητικές σε πόρους εργασίες τους και αυτές εκτελούνται, όποτε είναι δυνατό, από το σύστημα με κεντρική διαχείριση.
- *Συναλλαγών (transaction).* Εδώ υπάρχει συνεχής επικοινωνία χρήστη-συστήματος και η απόκριση θα πρέπει να δίνεται όσο πιο γρήγορα γίνεται. Αυτό το χαρακτηριστικό συναντάται και στα *διαλογικά (interactive)* συστήματα.
- *Μερισμού χρόνου (time sharing).* Το σύστημα διαμοιράζεται σε πολλούς χρήστες και είναι δυνατό να υπάρχει χρέωση για τις υπηρεσίες του.
- *Πραγματικού χρόνου (real time).* Το σύστημα πρέπει να εξασφαλίζει άμεση απόκριση σε προκαθορισμένο και συνήθως πολύ μικρό χρονικό διάστημα καθώς η λειτουργία του επηρεάζει κρίσιμες διαδικασίες όπως π.χ έλεγχος βιομηχανικών δραστηριοτήτων, έλεγχος αεροπλάνων, διαστημοπλοίων κτλ.
- *Ανοχής σφαλμάτων ή άνευ παύσης (fault tolerant ή non stop).* Εδώ πρόκειται για συστήματα τα οποία δεν επιτρέπεται να διακόψουν τη λειτουργία τους λόγω βλαβών υλικού ή άλλων λόγων. Προφανώς ένα σύστημα πραγματικού χρόνου θα πρέπει να παρέχει και αυτή τη δυνατότητα.
- *Κατανεμημένα (distributed).* Πρόκειται για συστήματα τα οποία έχουν γεωγραφική διασπορά των σταθμών εργασίας σε διάφορα σημεία.
- *Συστήματα πελάτη-εξυπηρετητή (client-server).* Αποτελούν την τελευταία εξέλιξη ενσωματώνοντας πολλά από τα παραπάνω χαρακτηριστικά. Πρόκειται για συστήματα όπου υπάρχει ένας ή περισσότεροι κεντρικοί υπολογιστές με επαυξημένες δυνατότητες (εξυπηρετητές/servers) οι οποίοι δέχονται απομακρυσμένες συνδέσεις από άλλους υπολογιστές (πελάτες/clients) και διαμοιράζουν υπολογιστικούς πόρους όπως αποθηκευτικό χώρο, εκτυπωτές κτλ και εφαρμογές όπως βάσεις δεδομένων, εφαρμογές γραφείου κτλ. Ο εξυπηρετητής και οι σταθμοί εργασίας (πελάτες) ελέγχονται συνήθως από διαφορετικά λειτουργικά συστήματα καθώς πρέπει να εξυπηρετήσουν διαφορετικές ανάγκες ο καθένας. Ενας νέος όρος στην Πληροφορική, η υπολογιστική νέφους (cloud computing) είναι μια ακόμα εξέλιξη ενός τέτοιου συστήματος που βασίζεται στη χρήση υπηρεσιών του παγκόσμιου ιστού και τη δυνατότητα χρήσης αποθηκευτικού χώρου και εφαρμογών δια μέσου του διαδικτύου.

**1.7.2 Κατάταξη με πλήθος χρηστών.** Ανάλογα με τον αριθμό των χρηστών που υποστηρίζουν τα λειτουργικά συστήματα διακρίνονται σε δύο κατηγορίες:

*Ενός Χρήστη (Single User).* Τα λειτουργικά συστήματα αυτά μπορούν να εξυπηρετήσουν μόνο ένα χρήστη σε κάθε χρονική στιγμή. Χαρακτηριστικά παραδείγματα τέτοιων λειτουργικών συστημάτων είναι τα Windows 95/98/2000, το MS-DOS και το Λειτουργικό Σύστημα των Apple Macintosh.

*Πολλών Χρηστών (Multiuser).* Τα λειτουργικά συστήματα αυτά μπορούν να εξυπηρετήσουν πολλούς χρήστες το ίδιο χρονικό διάστημα. Χαρακτηριστικά παραδείγματα τέτοιων λειτουργικών συστημάτων είναι τα Windows NT/2000/Server, το UNIX, το LINUX, το NOVELL,

το VMS της DEC, το OS/400 της IBM και τα λειτουργικά συστήματα των mainframes (IBM MVS, IBM VM, CDC NOS κ.λπ.).

**1.7.3 Κατάταξη με καθεστώς λειτουργίας.** Το καθεστώς λειτουργίας καθορίζεται από την ανάγκη ύπαρξης ή όχι μιας άδειας χρήσης του λογισμικού του λειτουργικού συστήματος η οποία έχει κάποιο κόστος. Όπως και σε πολλές κατηγορίες λογισμικού εφαρμογών, από τις αρχές της δεκαετίας του 90 και έπειτα με την ανάπτυξη και του διαδικτύου, υπάρχει μια νέα φιλοσοφία στην ανάπτυξη λογισμικού βασιζόμενη στη δημιουργία ανοιχτών κοινοτήτων ανάπτυξης λογισμικού. Σε αυτές τις κοινότητες η συμμετοχή είναι συνήθως εθελοντική. Ομάδες προγραμματιστών δουλεύουν σε κοινές εργασίες σχεδιασμού και ανάπτυξης λογισμικού. Αποτέλεσμα αυτών των δράσεων είναι η δημιουργία λογισμικού το οποίο παρέχεται για χρήση δωρεάν και ταυτόχρονα είναι διαθέσιμος και ο πηγαίος κώδικας του (Ελεύθερο Λογισμικό/Λογισμικό Ανοιχτού Κώδικα, ΕΛΛΑΚ). Συνήθως η μόνη υποχρέωση είναι η συνέχιση της δωρεάν παροχής σε περίπτωση περαιτέρω ανάπτυξης του, ενώ μπορεί να υπάρχει χρέωση για υποστήριξη στη χρήση αυτής της κατηγορίας λογισμικού. Εκπρόσωπος αυτού του τύπου λογισμικού στα λειτουργικά συστήματα είναι το LINUX το οποίο παρέχεται δωρεάν σε διάφορες εκδόσεις/διανομές και βασίζεται στη φιλοσοφία του UNIX.

## 1.8. Ιστορική Εξέλιξη των ΛΣ

Η ιστορική εξέλιξη των ΛΣ ακολούθησε την εξέλιξη της αρχιτεκτονικής των υπολογιστών. Για το λόγο αυτό τα ΛΣ μπορούν να κατηγοριοποιηθούν σε γενιές αντίστοιχες με τις γενιές των υπολογιστών όπως αναφέρεται παρακάτω:

**1η Γενεά (1945-1955): Η/Υ χωρίς ΛΣ.**

Ουσιαστικά οι πρώτοι υπολογιστές δεν είχαν Λειτουργικό Σύστημα. Αντ' αυτού οι χρήστες, οι οποίοι ήταν εξειδικευμένοι επιστήμονες – προγραμματιστές, έπρεπε να προγραμματίσουν την κάθε εργασία σε γλώσσα μηχανής ή ακόμα και με φυσικό χειρισμό διακοπτών.

**2η Γενιά (1955 – 1965)**

Με την ανακάλυψη και χρήση των τρανζίστορς (κρυσταλλοτρίοδοι) τα οποία αντικατέστησαν τις λυχνίες στους ηλεκτρονικούς υπολογιστές υπήρξε μια πρώτη μείωση του όγκου και αύξηση της λειτουργικότητας τους. Η ανάθεση εργασιών μπορεί να γίνει πλέον με χρήση διάτρητων καρτών το περιεχόμενο των οποίων περνούσε σε μαγνητικές ταινίες και από εκεί στη μνήμη του υπολογιστή ακολουθώντας μια αντίστροφη πορεία κατά την έξοδο των αποτελεσμάτων. Η χρήση των υπολογιστών συνεχίζει να απαιτεί εξειδίκευση και πολλές γνώσεις.

**3η Γενεά (1965 – 1980)**

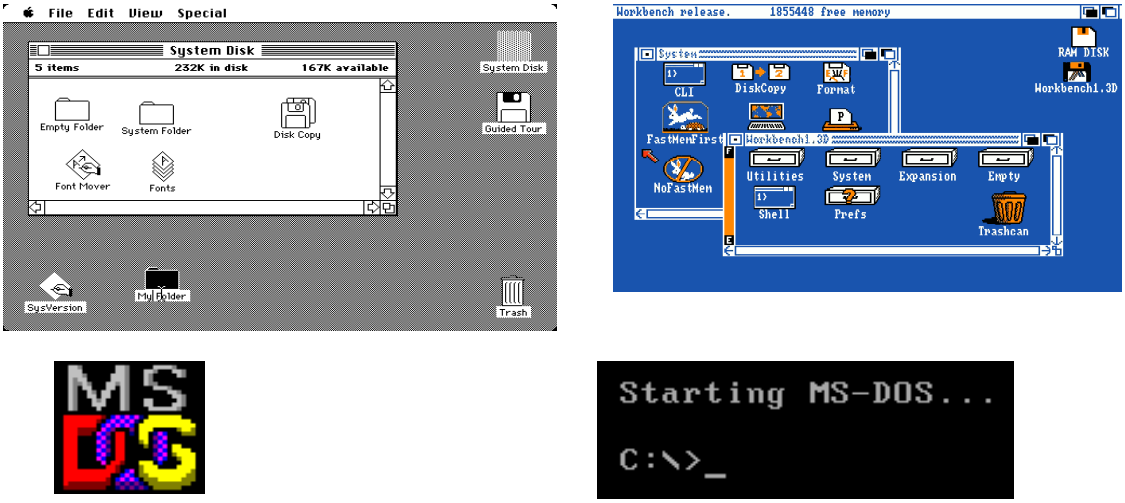
Σε αυτή τη γενεά εμφανίζονται σιγά σιγά τα χαρακτηριστικά που αναφέραμε στις κατηγορίες των λειτουργικών συστημάτων. Επινοούνται έννοιες όπως ο πολυπρογραμματισμός (multiprogramming) και η πολυδιεργασία (multitasking) που αναφέρονται στη δυνατότητα να συνυπάρχουν στη μνήμη και να εκτελούνται σταδιακά πολλά προγράμματα ή διεργασίες του ίδιου προγράμματος. Δημιουργούνται γλώσσες υποβολής εργασιών (Job Control Languages) και εμφανίζονται επίσης τερματικά για ευκολία στην διεπαφή και απομακρυσμένη πρόσβαση. Ο χρόνος των συστημάτων αυτών μπορεί πλέον να διαμοιραστεί σε πολλούς χρήστες οι οποίοι μπορούν να είναι ταυτόχρονα συνδεδεμένοι. Αυτή την περίοδο δημιουργείται το πρώτο UNIX σύστημα που καινοτομεί καθώς υπάρχει διαθέσιμο για διαφορετικούς τύπους υπολογιστών σε αντίθεση με τα λειτουργικά συστήματα που κατασκευάζονταν αποκλειστικά για έναν τύπο

υπολογιστή (π.χ VMS για τον VAX 11/750). Σαν περιβάλλον διεπαφής με τον χρήστη υπάρχουν πλέον οι διερμηνευτές εντολών.

**4η Γενεά (1980 – 1990)**

Το σημαντικό στοιχείο εδώ είναι η εμφάνιση των πρώτων προσωπικών υπολογιστών (IBM PC και συμβατά) οι οποίοι έχουν ως ΛΣ το MS-DOS της Microsoft. Παράλληλα υπάρχουν τα μεγάλα υπολογιστικά συστήματα (mainframes) που κάνουν χρήση του UNIX κυρίως αλλά και τα Macintosh της APPLE με το MAC-OS ως το Λειτουργικό Σύστημα με τις πρώτες χρήσεις γραφικού περιβάλλοντος επικοινωνίας.

Έννοιες όπως η φιλικότητα προς τον χρήστη αποκτούν σημασία και επιβάλλουν την ολοένα και μεγαλύτερη χρήση γραφικών όπως φαίνεται και στην εικ. 1.8. Αυτή τη περίοδο εμφανίζονται και τα λειτουργικά συστήματα δικτύου υπολογιστών (NOVELL).




Εικόνα 1.8: Λειτουργικά Συστήματα 4ης γενιάς

**5η Γενεά (1990 – σήμερα)**

Η ταχύτατη πλέον εξέλιξη της τεχνολογίας τόσο στο υλικό όσο και στο λογισμικό και η ανάπτυξη των δικτύων οδηγούν τις εξελίξεις. Προσωπικοί υπολογιστές αρχικά και προσωπικές έξυπνες συσκευές τα τελευταία χρόνια αποκτούν τεράστιες υπολογιστικές ικανότητες σε σύγκριση με τους υπολογιστές της $4^{ης}$ γενεάς. Τα λειτουργικά συστήματα εξελίσσονται και ενσωματώνουν τα περισσότερα από τα γνωρίσματα που έχουν σήμερα (φιλικότητα, πολυπρογραμματισμό, πολυχρησία, δικτύωση, ασφάλεια). Συστήματα πελάτη-εξυπηρετητή είναι το βασικό μοντέλο που ακολουθείται με κατάληξη όπως αναφέρθηκε και στην προηγούμενη παράγραφο τα σημερινά συστήματα νέφους (cloud computing) με χρήση του διαδικτύου.


Εικόνα 1.9: Λειτουργικά Συστήματα 5ης Γενιάς (εμπορικά σήματα)

## Ερωτήσεις

1. Ποια είναι η δομή των σύγχρονων Συστημάτων Υπολογιστών και γιατί;
2. Να αναφέρετε συνοπτικά τις κατηγορίες στις οποίες διακρίνεται το λογισμικό συστήματος. Σε ποια ευρύτερη κατηγορία εντάσσεται αυτό;
3. Ποιο ρόλο επιτελεί το Λειτουργικό Σύστημα σε έναν υπολογιστή; Τι θα γινόταν αν δεν υπήρχε αυτό;
4. Ποιες είναι οι βασικές αρμοδιότητες ενός λειτουργικού συστήματος;
5. Πώς επικοινωνεί ο χρήστης με το Λειτουργικό Σύστημα ;
6. Τι είναι ένα σύστημα Πολλών Χρηστών (Multiuser System);
7. Τι είναι ένα σύστημα Πολυδιεργασίας (Multitasking System);
8. Να αναφέρετε ονομαστικά τα κυριότερα μέρη ενός ΛΣ.
9. Τι γνωρίζετε για τον πυρήνα και το ρόλο του σε ένα ΛΣ;
10. Ποια είναι τα σημαντικότερα βήματα στην εξέλιξη των ΛΣ από την πρώτη γενιά μέχρι σήμερα;
11. Ποια είναι η διαφορά μεταξύ των όρων Πολυδιεργασίας (Multitasking) και Πολλών Χρηστών (Multiuser);
12. Ποιες ήταν ιστορικά οι κατηγορίες των λειτουργικών συστημάτων και ποιες καινοτομίες έφεραν;
13. Ποιες είναι οι τάσεις στο σχεδιασμό λειτουργικών συστημάτων από το 1980 και μετά ;
14. Να ορισθούν οι έννοιες Μερισμού χρόνου (Time sharing) και επεξεργασία Πραγματικού χρόνου (Real Time processing),
15. Σε ποιά κατηγορία λειτουργικών συστημάτων ανήκει το MS-DOS, τα Windows 98 και σε ποια το UNIX;

16. Να αναφέρετε τα πιο γνωστά ΛΣ. Τι γνωρίζετε για το καθένα;

17. Ποιες από τις παρακάτω εργασίες αποτελούν εργασίες του λειτουργικού συστήματος:
    1. Ορθογραφική διόρθωση κειμένου
    2. Διαμόρφωση δισκου
    3. Υποστήριξη εκτέλεσης πολλών διεργασιών ταυτόχρονα
    4. Μορφοποίηση παραγράφου
    5. Διαχείριση πόρων συστήματος

18. Ποια από τα παρακάτω αποτελούν μέρη ενός ΛΣ;
    1. Εκτυπωτής
    2. Σύστημα αρχείων
    3. Πληκτρολόγιο
    4. Διαχείριση μνήμης
    5. Οθόνη
    6. Διαχείριση ΚΜΕ

19. Επιλέξτε τις σωστές εκφράσεις :
    1. Το Λογισμικό χωρίζεται στο Λογισμικό Συστήματος και στο Λογισμικό Εφαρμογών.
    2. Το Λειτουργικό Σύστημα ασκεί ένα διακοσμητικό ρόλο δευτερεύουσας σημασίας στο υπολογιστικό μας σύστημα
    3. Ένα Λειτουργικό Σύστημα οδηγεί στην σπατάλη των πόρων του συστήματος
    4. Το αρχείο είναι μια νοητή μονάδα αποθήκευσης δεδομένων
    5. Ο πυρήνας ρυθμίζει την επικοινωνία των διεργασιών
    6. Όταν δύο επεξεργασίες ζητούν ταυτόχρονα την υλοποίησή τους από την ΚΜΕ τότε καταρρέει το σύστημα
    7. Το Λειτουργικό Σύστημα δεν λαμβάνει μέριμνα για προστασία και ασφάλεια
    8. Με την διαχείριση της μνήμης το ΛΣ μεταφέρει ολόκληρη τη μνήμη από τη μία επεξεργασία στην άλλη
    9. Στα συστήματα πραγματικού χρόνου είναι περιττό να τηρούνται οι χρονικοί περιορισμοί

## Δραστηριότητες

*(για Windows και Linux)*

1. Παρατηρήστε προσεκτικά και καταγράψτε τα βήματα που μεσολαβούν από τη στιγμή που πιέζετε το πλήκτρο ON/OFF του υπολογιστή σας μέχρι τη στιγμή που ο υπολογιστής είναι έτοιμος να δεχθεί εργασίες. Αν χρειαστεί να παγώσετε τη διαδικασία πατήστε το πλήκτρο Pause/Break.

2. Αναζητήστε στο διαδίκτυο τους όρους POST boot, BIOS, boot sequence, OS Loader, GRUB και συζητήστε σε ομάδες για την ερμηνεία τους.

3. Κατά την διαδικασία εκκίνησης των Windows πιέστε και βαστήξτε πατημένο το πλήκτρο F8 και εξετάστε τις επιλογές εκκίνησης.

4. Μόλις το Λειτουργικό είναι έτοιμο να δεχθεί εντολές εξοικειωθείτε με τη χρήση των εικονιδίων, ανοίξτε εφαρμογές, μετακινείστε και αλλάξτε μέγεθος στα παράθυρα τους.

5. Εξερευνήστε τις ιδιότητες του γραφικού περιβάλλοντος εργασίας που χρησιμοποιείτε. Δοκιμάστε να κάνετε δεξί κλικ πάνω σε μια θέση της επιφάνειας εργασίας και ελέγξτε τις δυνατότητες παραμετροποίησης και εξατομίκευσης που σας παρέχονται.

6. Εξερευνήστε τις εφαρμογές που είναι εγκατεστημένες στον υπολογιστή που εργάζεστε. Μπορείτε να τις κατατάξετε σε λογισμικό εφαρμογών και ειδικά εργαλεία;

7. Ελέγξτε την έκδοση του ΛΣ που χρησιμοποιείτε (στα Windows με δεξί κλίκ στο εικονίδιο «Ο Υπολογιστής μου» και μετά «Ιδιότητες», στο Ubuntu «Ρυθμίσεις Συστήματος»/«Λεπτομέρειες»)

8. Ανοίξτε ένα παράθυρο γραμμής εντολών και πληκτρολογήστε την εντολή HELP (εικ. 1.7).

9. Στα Windows XP ή 7 πληκτρολογήστε την εντολή MSCONFIG σε ένα παράθυρο γραμμής εντολών και εξερευνήστε τις δυνατότητες που σας παρέχονται. Αναζητήστε πληροφορίες για την εντολή στο διαδίκτυο.

# Κεφάλαιο 2

## Οργάνωση Συστήματος Αρχείων

Το αντικείμενο αυτού του κεφαλαίου είναι η οργάνωση του συστήματος αρχείων του υπολογιστή. Παρουσιάζονται έννοιες, όπως η διαχείριση αρχείων και το σύστημα αρχείων, αναλύεται η φυσική οργάνωση των αποθηκευτικών μέσων και αναφέρονται βασικά στοιχεία σχετικά με την ασφάλεια συστήματος.

### Διδακτικοί Στόχοι

Σε αυτό το κεφάλαιο θα μάθετε:

- Να χρησιμοποιείτε την ιεραρχική δομή αποθήκευσης αρχείων.
- Αναγνωρίζετε τις μονάδες αποθήκευσης δεδομένων (οπτικός δίσκος, σκληρός δίσκος, usb-flash, κ.λ.π).
- Για τα δικαιώματα χρηστών σε αρχεία και καταλόγους.
- Για την φυσική οργάνωση των αρχείων στον σκληρό δίσκο.
- Για την αναγκαιότητα της ασφάλειας συστήματος.

### Διδακτικές Ενότητες

2.1 Διαχείριση αρχείων και σύστημα αρχείων

2.2 Κατανομή των αρχείων σε συσκευές.

2.3 Φυσική οργάνωση του δίσκου

2.4 Προσπέλαση δίσκων

2.5 Ασφάλεια συστήματος

## 2.1. Διαχείριση Αρχείων και Σύστημα Αρχείων

**2.1.1. Εισαγωγή στη διαχείριση αρχείων.** Η ικανότητα αποθήκευσης δεδομένων είναι ένας από τους λόγους που συντέλεσαν στην εξάπλωση των Η/Υ σε εργασιακό και οικιακό χώρο.

Για να αποθηκευτούν δεδομένα σε Η/Υ, είναι απαραίτητο να τους δοθεί ένα όνομα (file name). Αυτό μπορεί να οριστεί ως **αρχείο, δηλαδή** ένα σύνολο από δεδομένα που είναι αποθηκευμένα με ένα όνομα. Δεδομένα όπως μουσική, ταινίες, κείμενα, φωτογραφίες και προγράμματα, αποθηκεύονται ως αρχεία σε συσκευές των Η/Υ. Οι συσκευές αυτές λέγονται **δευτερεύουσες** ή **βοηθητικές μνήμες** και η **αποθήκευση** σ' αυτές είναι **μόνιμη**, σε αντίθεση με την κύρια μνήμη RAM που η αποθήκευση είναι προσωρινή (μέχρι να κλείσει ο Η/Υ). Τέτοιες συσκευές αποθήκευσης είναι οι σκληροί δίσκοι (hard disks ή magnetic disks), οι οπτικοί δίσκοι (CD, DVD), μνήμες τύπου NAND όπως USB stisks και Solid State Drive (SSD), οι μαγνητικές ταινίες (magnetic tapes) και οι εύκαμπτοι δίσκοι (floppy disks).

Η μικρή ταχύτητα πρόσβασης είναι το κυριότερο μειονέκτημα των συσκευών δευτερεύουσας μνήμης (χιλιοστά δευτερολέπτου, msec=$10^{-3}$), σε σχέση με την κύρια μνήμη RAM (δισεκατομμυριοστά, nsec=$10^{-9}$), είναι δηλαδή πολλές χιλιάδες φορές μικρότερη.

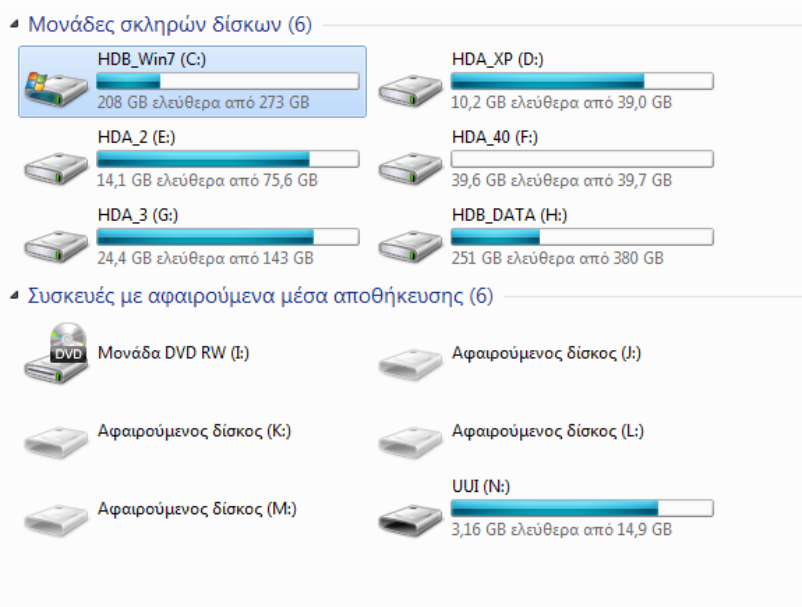

Εικόνα 2.1: Δευτερεύουσα μνήμη

**2.1.2 Σύστημα Αρχείων (File System).** Όταν ο χρήστης θέλει να αποθηκεύσει κάποιο αρχείο, το ΛΣ του ζητά μόνο το όνομα που θέλει να του δώσει. Από το σημείο εκείνο και μετά, ό,τι άλλο απαιτείται για να αποθηκευτεί το αρχείο το αναλαμβάνει το Λειτουργικό Σύστημα του Η/Υ.

Για να ελέγχει την αποθήκευση και την ανάκτηση αρχείων σε συσκευές, το ΛΣ χρησιμοποιεί ένα **Σύστημα Αρχείων** (file system). Κάθε Σύστημα Αρχείων οργανώνει (αποθηκεύει) τα αρχεία με την δική του λογική (τρόπο) και κρατά πληροφορίες γι' αυτά όπως: το όνομα, το μέγεθος, τον ιδιοκτήτη του, την ώρα και ημερομηνία δημιουργίας και τροποποίησης, τα δικαιώματα χρηστών και ομάδων και το *σημείο* της συσκευής που έχει αποθηκευτεί.

Υπάρχουν πολλά είδη Συστημάτων Αρχείων. Κάθε ΛΣ μπορεί να εγκατασταθεί σε συγκεκριμένα από αυτά και είναι πιθανό να μην έχει πρόσβαση σ' άλλα Συστήματα Αρχείων χωρίς πρόσθετες εφαρμογές τέτοιου σκοπού (πχ τα Windows χρειάζονται τέτοια εφαρμογή για να διαβάσουν

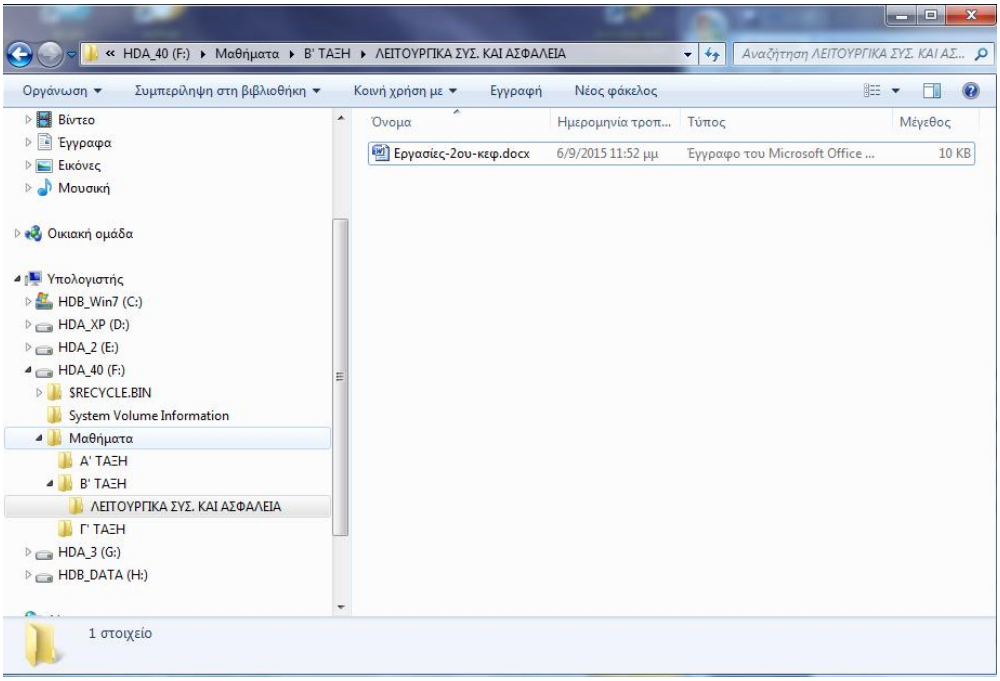
από ext3 σύστημα αρχείων). Γνωστότερα είδη Συστημάτων Αρχείων είναι: για Windows το **NTFS** και **FAT32**, για Linux (λίνουξ) το **ext3** και **ext4**, και για Mac Os X το **HFS+**.




Εικόνα 2.2: Απεικόνιση των αποθηκευτικών μέσων σε Η/Υ με ΛΣ Windows 7

**2.1.3 Ευρετήριο (Directory).** Σε κάθε Η/Υ υπάρχουν χιλιάδες αρχεία όπως κειμένων, προγραμμάτων, μουσικής και ταινιών. Αν αποθηκεύονταν όλα αυτά στον ίδιο χώρο, δε θα ήταν εύκολο να βρεθεί ένα συγκεκριμένο αρχείο ανάμεσά τους.

Όλα τα σύγχρονα ΛΣ χρησιμοποιούν τον **Ιεραρχικό** τρόπο οργάνωσης αρχείων για να μπορεί να γίνεται εύκολα η ταξινόμηση και εύρεσή τους. Σ' αυτόν, χρησιμοποιούνται ειδικά αρχεία που ονομάζονται **φάκελοι** (folders) ή **κατάλογοι** (catalogues) ή **ευρετήρια** (directories) και περιέχουν πληροφορίες για αρχεία (όνομα, μέγεθος, δικαιώματα, κ.λπ.) και άλλους φακέλους (**υποφακέλους**). Οι υποφάκελοι με τη σειρά τους μπορούν να περιέχουν πληροφορίες για άλλα αρχεία και υποφακέλους κ.λπ. Με αυτόν τον τρόπο δημιουργείται ένα **αντεστραμμένο δέντρο** όπου στην κορυφή του βρίσκεται η **ρίζα** (root) του δέντρου και κλαδιά του είναι οι φάκελοι που μπορούν να έχουν για παρακλάδια υποφακέλους.




Εικόνα 2.3: Παράδειγμα δομής φακέλων

**Για παράδειγμα**, στην εικ. 2.3 υπάρχει ο Διαχειριστής Αρχείων (**File Manager**) των Windows7. Στην αριστερή πλευρά της εικόνας κα κάτω από την λέξη *Υπολογιστής* βρίσκονται οι συσκευές Δευτερεύουσας μνήμης: C:, D:, E:, F:, G:, H:.

Κάτω από τη συσκευή F: (που έχει ως όνομα το HDA_40) υπάρχουν οι φάκελοι (κλαδιά δέντρου) *$RECYCLE.BIN*, *System Volume Information* και ***Μαθήματα***. Κάτω από τα *Μαθήματα* υπάρχουν οι υποφάκελοι (παρακλάδια) *Α' ΤΑΞΗ, Β' ΤΑΞΗ, Γ' ΤΑΞΗ* και κάτω από τον υποφάκελο *Β' ΤΑΞΗ* υπάρχει ο υποφάκελος *ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣ. ΚΑΙ ΑΣΦΑΛΕΙΑ*. Ο φάκελος *ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣ. ΚΑΙ ΑΣΦΑΛΕΙΑ* όπως φαίνεται και από τη Γραμμή Διευθύνσεων είναι επιλεγμένος με το ποντίκι. Όταν επιλέγεται από αριστερά ένας φάκελος, τότε αυτός λέγεται ***Τρέχων φάκελος*** (current) ή ***φάκελος Εργασίας*** (working), και στο δεξιό μέρος της οθόνης εμφανίζονται τα περιέχομενα αυτού του φακέλου που στο παράδειγμα είναι μόνο το αρχείο *Εργασίες-2ου-κεφ.docx*.

Στο παράδειγμα αυτό, η ρίζα είναι στο *HDA_40 (F:)* (συνήθως συμβολίζεται με \ σε Windows και με / σε Linux)

**2.1.4 Τι προσφέρει το Σύστημα Αρχείων.** Τα Σύστημα Αρχείων, και ανάλογα με το Λειτουργικό Σύστημα, παρέχουν του εξής μηχανισμούς χειρισμού αρχείων:

**Αρχεία οργάνωσης**. Αυτή γίνεται με τη χρήση φακέλων για να ομαδοποιηθούν τα αρχεία ανάλογα με: τον ιδιοκτήτη τους, τη συσκευή αποθήκευσης και με όποιον άλλο τρόπο επιθυμεί ο χρήστης.

**Αρχεία ονοματοδοσίας**. Σε κάθε ΛΣ υπάρχουν κάποιοι χαρακτήρες ή λέξεις που δεν επιτρέπεται η χρήση τους σε ονόματα αρχείων ή φακέλων.

*Δεν επιτρέπονται ή μπορεί να δημιουργήσει προβλήματα η χρήση τους*:

- Σε Windows: οι χαρακτήρες \ / ? : * " | > < έχουν ειδική χρήση από το ΛΣ τα ονόματα com1 και lpt1 μέχρι 9, CON, AUX NUL, PRN γιατί είναι ονόματα συσκευών
- Σε Linux: ο χαρακτήρας / (slash) και
  (Οι χαρακτήρες \ ? : * " | > < έχουν ειδική χρήση από το ΛΣ και ίσως δημιουργήσει προβλήματα η χρήση τους (κυρίως σε περίπτωση μεταφοράς τους) )

Το *μήκος ονομάτων* (filename length) είναι: για Windows 255 χαρακτήρες και για Linux 255 για ASCII χαρακτήρες και 64 για Unicode

*Επέκταση (extension) ή κατάληξη (suffix).* Στα ονόματα αρχείων μπορούν να χρησιμοποιηθούν μία η περισσότερες τελείες. Από την τελευταία τελεία και μετά υπάρχουν συνήθως 3 ή 4 χαρακτήρες, η επέκταση του αρχείου, που είναι μια ένδειξη για το περιεχόμενο του αρχείου και με τι είδους πρόγραμμα δημιουργήθηκε. Στον πίνακα 2.1 εμφανίζονται μερικές από τις γνωστότερες επεκτάσεις αρχείων.

| **Είδος αρχείου** | **Επέκταση** |
|---|---|
| Microsoft Word | docx |
| Microsoft Excel | xlsx |
| Microsoft PowerPoint | pptx |
| Adobe Portable Document Format | pdf |
| Shockwave Flash | swf |
| Αρχεία κειμένου | txt, rtf |
| Αρχεία εικόνας/γραφικών | gif, jpg, tiff, pict, png, mng |
| Αρχεία βίντεο | avi, dat, mpeg, swf, flv, Xvid, DivX, mov, mp4, 3pg |
| Αρχεία ήχου | wav, mp3, wma, m3u, mid |

Πίνακας 2.1 Οι πιο συνηθισμένες επεκτάσεις αρχείων

*Διάκριση πεζών-κεφαλαίων*.Στο ΛΣ Windows δεν γίνεται διάκριση πεζών-κεφαλαίων γραμμάτων πχ. τα λατινικά *A και a* είναι το ίδιο. Επομένως το αρχείο Abc.txt είναι το

ίδιο με το abc.txt και δεν μπορούν να υπάρχουν στον ίδιο φάκελο και τα δυο. Στο Linux γίνεται διάκριση πεζών-κεφαλαίων. Δηλαδή, το αρχείο *Abc.txt* είναι διαφορετικό από το *abc.txt* και μπορούν αν συνυπάρχουν στον ίδιο φάκελο.

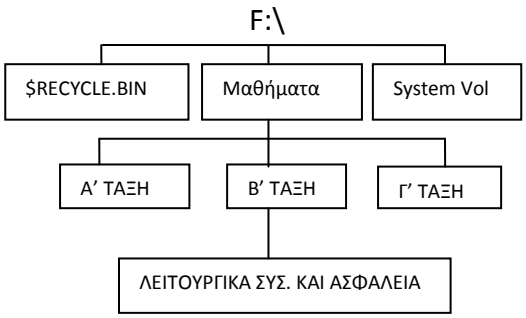
**Έλεγχο προσπέλασης.** Μπορούν να δοθούν /αφαιρεθούν δικαιώματα πάνω σ' ένα αρχείο για να προστατευτεί. Σε κάθε αρχείο καθορίζεται ο ιδιοκτήτης του και τα δικαιώματα που θα έχουν πάνω σ' αυτό οι υπόλοιποι χρήστες του ΛΣ. Ανάλογα με το Σύστημα Αρχείων και το ΛΣ, μπορούν να καθοριστούν διακιώματα: Εγγραφής (write), Ανάγνωσης (read), Διαγραφής (delete) και Εκτέλεσης (execute).

**Φυσικής αποθήκευσης**. Δίνεται η δυνατότητα να επιλεχθεί σε ποιά συσκευή βοηθητική μνήμης θα αποθηκευτεί ένα αρχείο. Διαφορετικές συσκευές μπορούν να έχουν διαφορετικά συστήματα αρχείων επομένος και τρόπο εγγραφής τους.

**Απόλυτη (absolute) και Σχετική (relative) αναφορά σε αρχείο.** Η θέση ενός αρχείου προσδιορίζεται από το μονοπάτι ή διαδρομή (pathname) προς αυτό. Το διαχωριστικό φακέλων σε Windows είναι το σύμβολο \, ενώ σε Linux είναι το σύμβολο /. Στο παράδειγμα της εικ. 2.3 η διαδρομή προς το αρχείο *Εργασίες-2ου-κεφ.docx* είναι:

F:**** Μαθήματα **** Β' ΤΑΞΗ **** ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣ. ΚΑΙ ΑΣΦΑΛΕΙΑ **** Εργασίες-2ου-κεφ.docx

Όταν η διαδρομή αναφοράς προς ένα αρχείο ξεκινά από την αρχή του δέντρου (ρίζα) λέγεται ***Απόλυτη*** διαδρομή και υπάρχει *για κάθε αρχείο μόνο μία* τέτοια διαδρομή και αρχίζει **πάντα** με \ (back slash) σε Windows και / (slash) σε Linux.




Ο **γονικός** φάκελος ενός υποφακέλου λέγεται ο ιεραρχικά ανώτερος φάκελος και συμβολίζεται με *δυο συνεχόμενες τελείες* **..**. Έτσι, ο γονικός φάκελος του *ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣ. ΚΑΙ ΑΣΦΑΛΕΙΑ* είναι ο *Β' ΤΑΞΗ*, του *Β' ΤΑΞΗ* είναι ο φάκελος *ΜΑΘΗΜΑΤΑ* και του *ΜΑΘΗΜΑΤΑ* είναι η ρίζα \.

Εκτός από την Απόλυτη υπάρχει και η **Σχετική** αναφορά διαδρομής προς ένα αρχείο. Σ' αυτήν, η αναφορά γίνεται σε σχέση με τον **τρέχοντα (εργασίας) φάκελο** τη στιγμή της αναφοράς. Στο παράδειγμα της ενότητας 2.1.3 και στην εικ. 2.3, φάκελος εργασίας είναι ο ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣ. ΚΑΙ ΑΣΦΑΛΕΙΑ.

**Παράδειγμα:** έστω πως στον φάκελο Α' ΤΑΞΗ υπάρχει το αρχείο *abc.jpg* και θέλουμε να κάνουμε σχετική αναφορά προς αυτό το αρχείο.

Για μια σχετική αναφορά (μπορεί να υπάρχουν πολλές) προς το αρχείο *abc.jpg* από τον *τρέχον* φάκελο θα πρέπει να λάβουμε υπόψη τα εξής: τρέχον φάκελος είναι ο ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣ. ΚΑΙ ΑΣΦΑΛΕΙΑ. Για να βρεθούμε στον φάκελο Α' ΤΑΞΗ θα πρέπει να φτάσουμε στον φάκελο ΜΑΘΗΜΑΤΑ γιατί κάτω από αυτόν βρίσκεται ο Α' ΤΑΞΗ. Για να πάμε στον φάκελο ΜΑΘΗΜΑΤΑ πρέπει να περάσουμε μέσα από τον Β' ΤΑΞΗ.

.. **** .. **** Α' ΤΑΞΗ **** abc.jpg *(σε Windows)* και .. **/** .. **/** Α' ΤΑΞΗ **/** abc.jpg *(σε Linux)*

.. (*γονικός του ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣ. ΚΑΙ ΑΣΦΑΛΕΙΑ για να πάμε στον Β' ΤΑΞΗ*) **** .. (*γονικός του Β' ΤΑΞΗ για να πάμε στον φάκελο ΜΑΘΗΜΑΤΑ*) **** *Α' ΤΑΞΗ* (*για να μπούμε στον υποφάκελο του ΜΑΘΗΜΑΤΑ που βρίσκεται το αρχείο*) **** abc.jpg

Κάθε Λειτουργικό Σύστημα *διαθέτει* ***εντολές*** που μπορούν να δοθούν από το πληκτρολόγιο (γραμμή εντολών) ή με ενέργειες του ποντικιού μέσα από το πρόγραμμα Διαχείρισης Αρχείων (file manager), με τις οποίες μπορεί να κάνει διάφορους *χειρισμούς* σε *αρχεία* και *φακέλους*. Τέτοιες ενέργεις και χειρισμοί που γίνονται με εντολές είναι :

- Αναζήτηση Αρχείου
- Εκτέλεση Προγράμματος
- Δημιουργία Αρχείου
- Διαγραφή αρχείου
- Αντιγραφή αρχείου
- Αλλαγή Ονόματος αρχείου
- Δημιουργία Ευρετηρίου
- Καταστροφή Ευρετηρίου
- Παραχώρηση Δικαιωμάτων Προσπέλασης
- Αφαίρεση Δικαιωμάτων Προσπέλασης

Οι εντολές αυτές, συχνά διαφέρουν από ΛΣ σε ΛΣ τόσο ως προς την ίδια την εντολή αλλά και ως προς την σύνταξή της. Παραδείγματα χρήσης τους υπάρχουν στο σχολικό βιβλίο στις σελίδες:

- 37-42 για Windows
- 137-154 για γραμμή εντολών Linux-Unix

**2.1.5 Τύποι αρχείων.** Όπως είδαμε στον πίνακα 2.1, τα αρχεία, ανάλογα με το περιεχόμενό τους, έχουν και κάποια επέκταση. Γενικά υπάρχουν οι παρακάτω τύποι αρχείων:

**Αρχεία Δεδομένων (Data Files):** περιέχουν πληροφορίες που μπορούν να διαχειριστούν ειδικά προγράμματα. Παραδείγματα: ένα αρχείο με επέκταση .mp3 περιέχει μουσική και μπορεί κάποιος να ακούσει το περιεχόμενό του με προγράμματα αναπαραγωγής μουσικής.

**Αρχεία Κειμένου (Text Files):** Είναι απλά αρχεία κειμένου με περιεχόμενο μόνο χαρακτήρες ASCII ή UNICODE. Αυτά μπορούν να εμφανιστούν χωρίς ειδικά προγράμματα ακόμα και από την γραμμή εντολών.

**Αρχεία Προγραμμάτων (Program Files):** περιέχουν εντολές σε γλώσσα μηχανής (0 και 1). Δε διαβάζονται, ούτε εκτυπώνονται.

**Αρχεία Συστήματος (System Files):** είναι ειδικά αρχεία που χρησιμοποιούνται μόνο από το ΛΣ.

**Αρχεία Συσκευών (Device Files):** είναι συσκευές του συστήματος (εκτυπωτές, δίσκοι, κ.λπ.) που εμφανίζονται από το Λειτουργικό Σύστημα ως απλά αρχεία.

**Προσωρινά Αρχεία (Temporary Files):** δημιουργούνται για προσωρινή αποθήκευση και καταστρέφονται από το Λειτουργικό Σύστημα ή το πρόγραμμα που τα χρησιμοποιεί όταν δεν χρειάζονται πλέον.

**Αρχεία Εκτύπωσης (Printer, Spooler Files):** είναι βοηθητικά αρχεία για να εκτυπωθεί ό,τι έχει σταλεί στον εκτυπωτή.

**Εφεδρικά Αρχεία (Backup Files):** είναι αντίγραφα σημαντικών αρχείων που αποθηκεύονται σε διαφορετική συσκευή για να προστατευτούν από καταστροφή.

**Αρχεία Δέσμης Εντολών (Batch Files):** είναι απλά αρχεία κειμένου που περιέχουν πολλές εντολές του ΛΣ. Βοηθούν τους χρήστες γιατί, δίνοντας αυτός μια εντολή για να εκτελεστεί το Αρχείο Δέσμης, εκτελούνται όλες όσες περιέχει το αρχείο αυτό.

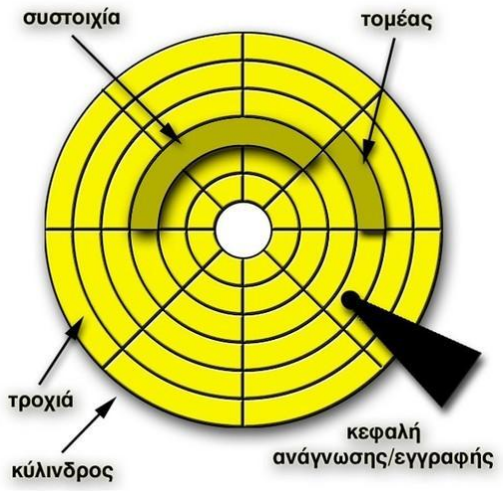
## 2.2 Κατανομή των αρχείων σε συσκευές.

Τα αρχεία ενός Η/Υ μπορούν να αποθηκευτούν σε κάποια από τις συνδεδεμένες συσκευές δευτερεύουσας μνήμης. Η επιλογή της συσκευής που θα αποθηκευτούν τα αρχεία γίνεται με κάποιο σκεπτικό:

- Αν χρειάζονται συχνά στους χρήστες, τότε είναι προτιμότερο να αποθηκεύονται σε κάποιο σκληρό δίσκο γιατί έχουν μεγάλη ταχύτητα μεταφοράς δεδομένων.
- Όταν υπάρχουν πολλοί δίσκοι, τα αρχεία μπορούν να μοιράζονται σ' αυτούς, για να μην υπάρχουν καθυστερήσεις όταν δίνονται ταυτόχρονα πολλές εντολές για ανάγνωση ή εγγραφή αρχείων.
- Μεγάλα αρχεία ή σπάνια χρησιμοποιούμενα, μπορούν να αποθηκεύονται σε μέσα που είναι φτηνότερα και έχουν μεγάλη χωρητικότητα (μαγνητικές ταινίες, αλλά και σκληρούς δίσκους).
- Τα αντίγραφα ασφαλείας μπορούν γράφονται σε μαγνητικές ταινίες ή σκληρούς δίσκους και φυλάγονται σε ασφαλές μέρος. Απλοί χρήστες μπορούν να χρησιμοποιήσουν και CD/DVD αν επαρκεί ο χώρος τους.

## 2.3 Φυσική Οργάνωση του δίσκου

Πριν τη χρήση του δίσκου θα πρέπει αυτός να οργανωθεί κατάλληλα από το Λειτουργικό Σύστημα, έτσι ώστε να υπάρχουν σημάδια για να μπορούν να βρεθούν οι αποθηκευμένες πληροφορίες. Τα σημάδια αυτά γράφονται με μαγνητικό τρόπο και χωρίζουν τον κάθε δίσκο σε ομόκεντρες **τροχιές ή ίχνη (tracks)** και **τομείς (sectors)** ανά τροχιά όπως φαίνεται στην εικ.2.5. Μια ομάδα από τομείς καλείται **συστοιχία (cluster)** (ή μονάδα εκχώρησης σε νεότερη ορολογία), ενώ οι αντίστοιχες τροχιές από κάθε επιμέρους δίσκο σε ένα σκληρό δίσκο συνιστούν έναν **κύλινδρο (cylinder).** Η διαδικασία δημιουργίας της παραπάνω δομής σε ένα σκληρό δίσκο καλείται **μορφοποίηση (format) ή διαμόρφωση** και είναι απαραίτητο να γίνει πριν ο δίσκος μπορέσει να χρησιμοποιηθεί.

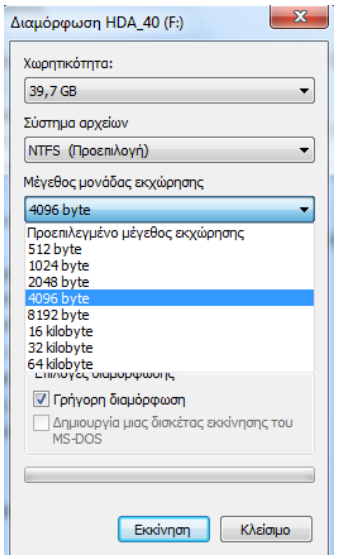



Εικόνα 2.5: Φυσική οργάνωση του μέσου αποθήκευσης. *(πηγή: βιβλιογραφία #9*)

Η συστοιχία είναι η μικρότερη περιοχή του δίσκου που μπορεί να αποδοθεί σε ένα αρχείο. Το πλήθος των τομέων που συνιστούν μια συστοιχία ορίζεται κατά την μορφοποίηση (διαμόρφωση) (βλ. εικ.2.5 και εικ.2.6) και είναι συνήθως 1, 2, 4, 8, 16, 32 ή 64 τομείς. Το μέγεθος μιας συστοιχίας σε bytes ορίζει και το μέγεθος του μπλοκ δεδομένων που μεταφέρεται σε κάθε λογική διαδικασία ανάγνωσης/εγγραφής στον δίσκο.

Επειδή το πλήθος των bytes σε κάθε τομέα είναι σταθερό και επίσης το πλήθος των τομέων ανά τροχιά είναι σταθερό θα πρέπει το πλήθος των bytes και ανά τροχιά να είναι σταθερό. Αυτό σημαίνει ότι οι εσωτερικές, προς το κέντρο, τροχιές είναι πιο πυκνογραμμένες από τις εξωτερικές. Αυτό όμως σημαίνει επίσης ότι υπάρχει αναξιοποίητος χώρος στον δίσκο και αντιμετωπίζεται πλέον με μια νέα τεχνολογία που ονομάζεται *Zone Bit Recording (ZBR).* Αυτή επιτρέπει να υπάρχουν περισσότεροι τομείς στις εξωτερικές τροχιές χωρίζοντας τον δίσκο σε ζώνες που περιέχουν περισσότερες από μια τροχιές. Οι τροχιές που βρίσκονται εντός μιας ζώνης έχουν τον ίδιο αριθμό τομέων αλλά καθώς μετακινούμαστε προς την εξωτερική πλευρά του δίσκου ο αριθμός αυτός αυξάνει.

Με τα παραπάνω στοιχεία, για να προσδιοριστεί η θέση μιας ομάδας δεδομένων απαιτούνται η επιφάνεια (ποιος από τους δίσκους που απαρτίζουν τον σκληρό δίσκο δηλαδή), το ίχνος (τροχιά), η συστοιχία (μονάδα εκχώρησης) και ο τομέας (ομάδα). Αυτά τα στοιχεία καλούνται και διεύθυνση της ομάδας.




Εικόνα 2.6: Επιλογές διαμόρφωσης στα Windows 7

### 2.3.1 Χωρισμός δίσκου σε διαμερίσματα

Αν προσέξουμε την εικ. 2.2 θα παρατηρήσουμε ότι απεικονίζονται έξι μονάδες σκληρών δίσκων. Στην πραγματικότητα οι σκληροί δίσκοι είναι μόνο δύο αλλά είναι χωρισμένοι ο πρώτος σε τέσσερα και ο δεύτερος σε δύο διαμερίσματα (partitions). Το γεγονός αυτό απεικονίζεται αναλυτικά στην εικ. 2.8. Η διαδικασία δημιουργίας των διαμερισμάτων (ή τόμων, volumes) λέγεται διαμερισμός (partitioning) και είναι ένας εικονικός διαχωρισμός του δίσκου σε δύο ή περισσότερα τμήματα.

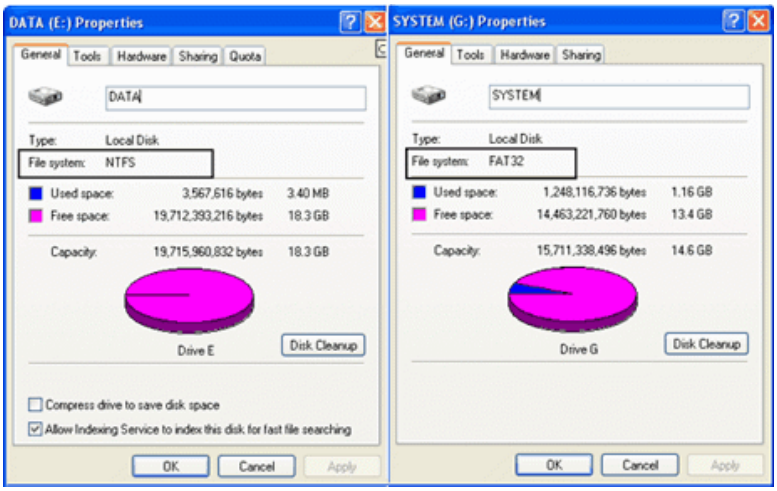
Όμως, όλα τα τμήματα δεν παύουν να είναι μέρος του ίδιου δίσκου. Αυτό σημαίνει πως, αν ο σκληρός δίσκος χαλάσει, τα δεδομένα όλων των διαμερισμάτων θα χαθούν.

Η χρήση των διαμερισμάτων δίσκου είναι σημαντική για λόγους οργάνωσης, προστασίας και διαχωρισμού των δεδομένων μεταξύ τους και χρήσης περισσοτέρων του ενός Λειτουργικών Συστημάτων και Συστημάτων Αρχείων στον υπολογιστή μας. Επίσης ανάλογα με τον σκοπό χρήσης του διαμερίσματος μπορούμε να ορίσουμε διαφορετικό μέγεθος μονάδας εκχώρησης (δηλαδή διαφορετικό πλήθος τομέων ανά συστοιχία για κάθε διαμέρισμα του δίσκου).

### 2.3.2 Είδη συστημάτων αρχείων

Είδαμε ότι, για να μπορέσει να δημιουργηθεί η παραπάνω δομή και να χρησιμοποιηθεί ένας δίσκος, είναι απαραίτητη η διαδικασία μορφοποίησης. Η μορφοποίηση καθορίζει εκτός από τα παραπάνω χαρακτηριστικά (ίχνη, τομείς, κτλ), και τον τύπο του συστήματος αρχείων που θα χρησιμοποιηθεί. Ο τύπος αυτός καθορίζει πώς θα υλοποιηθεί η δομή αρχείων που περιγράφηκε στις πρώτες ενότητες και τι δυνατότητες θα έχει.

Τα επικρατέστερα συστήματα αρχείων που χρησιμοποιούν τα Windows είναι το FAT στις διάφορες εκδοχές του – FAT12, FAT16, FAT32- και το NTFS. Στα λειτουργικά συστήματα που βασίζονται στο Unix (π.χ Linux) υπάρχουν αντίστοιχα συστήματα αρχείων όπως το UFS (Unix File System) τα ext2, ext3, ext4 και άλλα.




Εικόνα 2.7: Απεικόνιση του τύπου του συστήματος αρχείων.

**FAT/FAT32 - File Allocation Table**

Το FAT αναπτύχθηκε από τη Microsoft το 1977. Είναι ιδανικό για μικρού μεγέθους δίσκους καθώς καταλαμβάνει λιγότερο χώρο για τις οργανωτικές του πληροφορίες από το NTFS. Επίσης το FAT (που υπάρχει σε διάφορες εκδόσεις όπως FAT12, FAT16, FAT32) είναι πιο εύκολα αναγνωρίσιμο από άλλα λειτουργικά συστήματα εκτός των Windows (όπως Unix, Mac OS, Linux, FreeBSD κ.λπ.).

Το βασικό μειονέκτημα του FAT και του FAT32 είναι πως δεν μπορούν να διαχειριστούν αρχεία μεγαλύτερα των 2 GB και 4 GB αντίστοιχα, ενώ έχουν τον περιορισμό των 32GB στο μέγεθος των διαμερισμάτων ( partitions) που μπορεί να διασπασθεί ο δίσκος.

**NTFS - New Technology File System**

Το NTFS αναπτύχθηκε το 1993, ταυτόχρονα με την πρώτη έκδοση των Windows NT.

Ο τύπος αυτός λύνει ουσιαστικά όλους τους περιορισμούς μεγέθους αρχείων και διαμερισμάτων που έχουν τα FAT. Ετσι, το μεγαλύτερο αρχείο που μπορεί να υποστηρίξει το NTFS έχει μέγεθος 1 Exabyte (1 δισεκατομμύριο Gigabytes), ενώ μπορεί να δημιουργήσει διαμέρισμα δίσκου μεγέθους $2^{64}$ clusters.

Στην πράξη, το μεγαλύτερο partition που υποστηρίζεται αυτή τη στιγμή είναι 256 Terabytes. Επίσης, τα Windows 7 μπορούν να αναγνωρίσουν ένα αρχείο με μέγεθος μέχρι 16 Terabytes, ενώ τα Windows 8 μέχρι 256 Terabytes.

Το NTFS μπορεί επίσης να διαχειριστεί καλύτερα τον ελεύθερο χώρο σε σχέση με τα FAT και FAT32 και ο κατακερματισμός αρχείων (fragmentation) που θα δούμε παρακάτω, είναι μικρότερος. Επιπλέον, το NTFS παρέχει περισσότερες δυνατότητες και χαρακτηριστικά ασφαλείας όπως π.χ ορισμό δικαιωμάτων πρόσβασης και δυνατότητες κρυπτογράφησης και συμπίεσης.

**exFAT (FAT64) - Extended File Allocation Table**

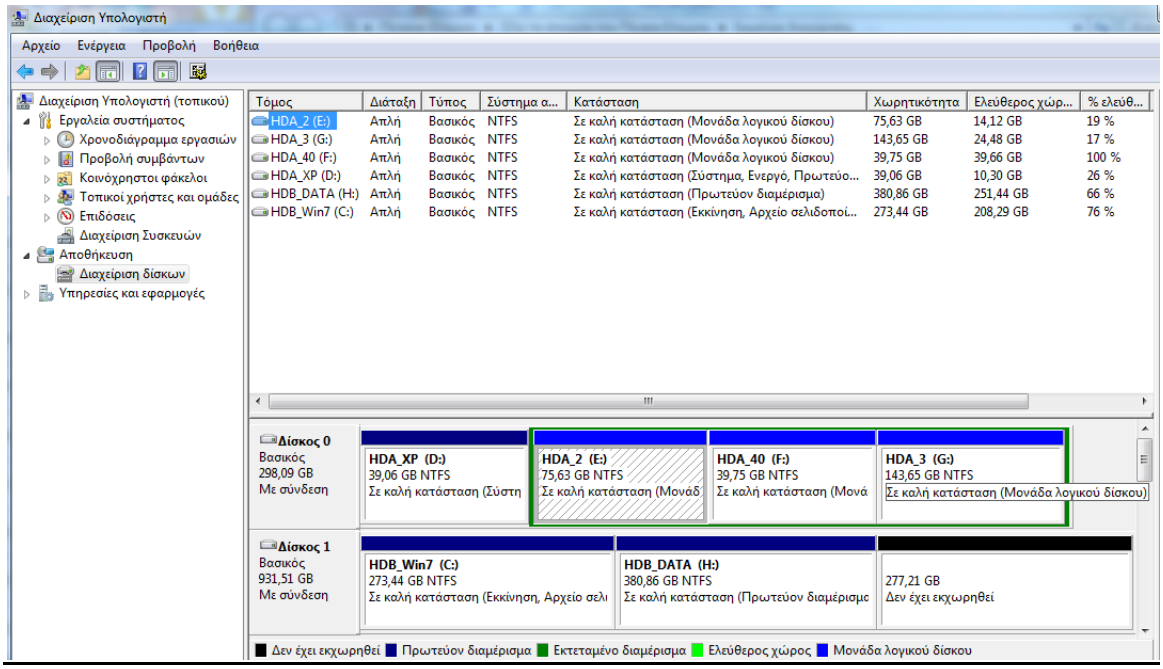
Το exFAT είναι ένα σύστημα της Microsoft σχεδιασμένο για μνήμες flash. Χρησιμοποιείται εκεί που ούτε το NTFS είναι καλή λύση (γιατί χρησιμοποιεί πολλά δεδομένα διαχείρισης του συστήματος αρχείων) άλλα ούτε και το FAT, λόγω των περιορισμών μεγέθους που είδαμε παραπάνω.

Το μέγιστο θεωρητικό μέγεθος αρχείου που υποστηρίζει είναι 16 Exabytes, ενώ το μέγιστο Partition είναι 64 Zettabytes (=τρισεκατομμύρια gigabytes).

Το exFAT έχει εφαρμοστεί σε ορισμένα μοντέλα USB flash, καθώς επίσης και σε τηλεοράσεις, media centers και φορητούς media players. Όμως καθώς προστατεύεται από πατέντες η υποστήριξή του πέραν των Windows και του MAC OS είναι περιορισμένη, και οι περισσότερες συσκευές συνεχίζουν να χρησιμοποιούν τα FAT/FAT32.

**ext2, ext3, ext4 – Second/Thirs/Fourth extended file systems**

Τα συστήματα αυτά χρησιμοποιούνται από τα συστήματα Linux όπως αναφέρθηκε παραπάνω και στη τελευταία έκδοση τους (το ext4) υποστηρίζουν 1 Exabyte χωρητικότητα και μεγέθη αρχείων μέχρι και 16 Terabytes ενώ δεν έχουν περιορισμό στο πλήθος των καταλόγων και προσφέρουν δυνατότητα ανασυγκρότησης κατά τη λειτουργία.




Εικόνα 2.8: Απεικόνιση του διαμερισμού των δίσκων σε ένα σύστημα υπολογιστή.

## 2.4 Προσπέλαση δίσκων

Η διαδικασίες ανάγνωσης ή εγγραφής σε ένα δίσκο γίνονται πάντα μέσω κλήσεων του λειτουργικού συστήματος. Αυτό δεν είναι πάντα προφανές σε έναν προγραμματιστή που γράφει ένα πρόγραμμα σε γλώσσα υψηλού επιπέδου άλλα όλες οι απαιτήσεις ανάγνωσης/εγγραφής (I/O Requests) μεταφράζονται τελικά σε κλήσεις του λειτουργικού συστήματος.

Οι απαιτήσεις αυτές αποτελούνται από τα παρακάτω στοιχεία:

- Εντολή (Read,Write, κ.λπ.)
- Λογική Συσκευή (C:, sda κτλ)
- Λογική διεύθυνση ομάδας δεδομένων (1η, 2η, 3η ...)
- Φυσική διεύθυνση ομάδας (τη βρίσκει το Λειτουργικό Σύστημα)
- Αριθμός ομάδων δεδομένων (blocks) που θα μεταφερθούν

Οι απαιτήσεις αυτές συγκεντρώνονται σε ουρές (Queues) για κάθε αποθηκευτικό μέσο και εξυπηρετούνται με κάποια σειρά.

Ο χρόνος που αναλώνεται από ένα πρόγραμμα στις διαδικασίες εγγραφής/ανάγνωσης αποτελεί το μεγαλύτερο ποσοστό καθυστέρησης στην εκτέλεση του. Ιδίως όταν το πρόγραμμα κάνει εντατική χρήση των αποθηκευτικών μέσων (I/O intensive). Σε τέτοιες περιπτώσεις εχει παρατηρηθεί ότι το 90% της καθυστέρησης οφείλεται σε αυτό τον λόγο και μόνο το 10% στην αναμονή χρήσης της ΚΜΕ. Αυτό οφείλεται στη μεγάλη διαφορά ταχύτητας λειτουργίας των αποθηκευτικών μέσων σε σχέση με την κύρια μνήμη και την ΚΜΕ. Οι παράγοντες της καθυστέρησης αναφέρονται παρακάτω:

- **Ο χρόνος αναμονής** στην ουρά μέχρι να αρχίσει η εξυπηρέτηση (Wait Time)
- **Ο χρόνο αναζήτησης του ίχνους** (track) από την κεφαλή (head) του δίσκου (Seek Time)
- **Ο χρόνος περιστροφής** και καθυστέρησης του δίσκου μέχρι η κεφαλή να έλθει πάνω από το ζητούμενο τομέα (Rotational Delay ή Latency Time)
- **Ο χρόνος μεταφοράς** των blocks (Transfer Time) από ή προς το δίσκο.

Όπως είναι φυσικό, στόχος του λειτουργικού συστήματος, εκτός από την αξιόπιστη διεκπεραίωση των αιτημάτων εγγραφής/ανάγνωσης είναι και η ελαχιστοποίηση του χρόνου καθυστέρησης.

### 2.4.1 Καταχώρηση περιοχών του δίσκου.

Όταν φτάσει η στιγμή να δημιουργηθεί ένα αρχείο, το Λειτουργικό Σύστημα το αποθηκεύει σε μονάδες εκχώρησης (συστοιχίες, clusters). Κάθε αρχείο έχει τουλάχιστον μια μονάδα εκχώρησης. Αυτό σημαίνει ότι, αν η μονάδα εκχώρησης έχει μέγεθος 4096 bytes και το αρχείο έχει περιεχόμενο έναν χαρακτήρα (δηλαδή 1 byte), τότε ο χώρος που θα καταλαμβάνει το αρχείο στον δίσκο θα είναι 4096 bytes. Τα υπόλοιπα 4095 bytes λοιπόν δεν θα αξιοποιούνται. Αυτό ονομάζεται *εσωτερικός κατακερματισμός (internal fragmentation)* του δίσκου.

Η απόδοση των μονάδων εκχώρησης (blocks, μπλοκ) στα αρχεία γίνεται με διάφορους τρόπους οι οποίοι αναφέρονται παρακάτω.

**Συνεχής καταχώρηση (Contiguous Allocation)**

Στην καταχώρηση αυτή τα μπλοκ του αρχείου είναι συνεχόμενα στον δίσκο. Αυτό έχει το πλεονέκτημα ότι είναι απλό στην υλοποίηση και ότι για κάθε αρχείο απαιτείται μόνο η διεύθυνση του πρώτου μπλοκ. Το μειονέκτημα είναι ότι το μέγεθος των αρχείων δεν είναι πάντα γνωστό κατά τη στιγμή της δημιουργίας τους και το σύστημα δεν γνωρίζει πόσο χώρο να δεσμεύσει.

**Καταχώρηση συνδεδεμένης λίστας (Linked List Allocation)**

Σε αυτή τη μέθοδο το αρχείο καταχωρείται ως μια συνδεδεμένη λίστα από μπλοκ. Στο τέλος του πρώτου μπλοκ τοποθετείται ο αριθμός του επόμενου μπλοκ (ένας δείκτης δηλαδή στο επόμενο μπλοκ) και το τελευταίο μπλοκ έχει μια ειδική τιμή για να δείξει το τέλος της

αλυσίδας. Ένα μειονέκτημα αυτής της μεθόδου είναι ότι δεν είναι δυνατή η άμεση προσπέλαση σε κάποιο τμήμα του αρχείου καθώς δεν είναι γνωστές οι διευθύνσεις των μπλοκ.

**Καταχώρηση με χρήση δείκτη (Indexed Allocation)**

Αυτή είναι μια παραλλαγή της μεθόδου συνδεδεμένης λίστας στην οποία διατηρείται ένας πίνακας όπου υπάρχει μια θέση για κάθε μπλοκ του δίσκου (FAT, File Allocation Table). Ετσι, το περιεχόμενο της θέσης του πίνακα που αντιστοιχεί στο πρώτο μπλοκ του αρχείου θα είναι η διεύθυνση του δεύτερου μπλοκ του αρχείου κ.ο.κ. Στη θέση του τελευταίου μπλοκ υπάρχει επίσης μια ειδική τιμή που σηματοδοτεί το τέλος του αρχείου. Όπως φαίνεται και από το όνομα του πίνακα αυτή η μέθοδος χρησιμοποιείται στα συστήματα FAT που είδαμε παραπάνω.

**Κόμβοι-δ (i-nodes)**

Η μέθοδος αυτή στηρίζεται πάλι στη χρήση δεικτών αλλα με διαφορετικό τρόπο. Έτσι, για κάθε αρχείο υπάρχει ένας μικρός πίνακας που λέγεται δ-κόμβος (i-node) και αυτός περιέχει τους αριθμούς των μπλοκ του αρχείου. Σε περίπτωση μεγάλων αρχείων όπου ο πίνακας δεν είναι αρκετός για να χωρέσει όλες τις θέσεις των μπλόκ, μια θέση του πίνακα αυτού περιέχει την διεύθυνση έναν άλλου πίνακα που περιέχει τις υπόλοιπες θέσεις. Σε αυτή τη λογική στηρίζονται τα συστήματα ext2, ext3, ext4 που είδαμε παραπάνω. Επίσης το σύστημα NTFS υλοποιεί κάτι ανάλογο με τη χρήση του Master File Table (MFT).

**2.4.2 Κατακερματισμός (Fragmentation).** Μετά από πολλές διαδικασίες δημιουργίας και διαγραφής αρχείων είναι αναμενόμενο ότι τα μπλοκ του κάθε αρχείου θα βρίσκονται διασκορπισμένα στον δίσκο. Αυτό θα έχει ως αποτέλεσμα οι φυσικές διαδικασίες ανάγνωσης/εγγραφής να απαιτούν πολλές μετακινήσεις των κεφαλών του σκληρού δίσκου έτσι ώστε να βρεθούν στις κατάλληλες θέσεις. Έτσι όμως αυξάνεται ο χρόνος που απαιτείται για την ανάγνωση/εγγραφή. Αυτή η κατάσταση ονομάζεται *εξωτερικός κατακερματισμός (external fragmentation)* και μειώνει την απόδοση του δίσκου. Για την αντιμετώπιση του είναι δυνατό να γίνει μια λειτουργία ανασυγκρότησης (αποκατακερματισμού, defragmentation) του δίσκου όπου τα μπλοκ των αρχείων τοποθετούνται σε γειτονικές θέσεις στο μεγαλύτερο δυνατό βαθμό. Η λειτουργία αυτή είναι καλό να γίνεται τακτικά σε κάθε δίσκο ενός υπολογιστικού συστήματος.

## 2.5 Ασφάλεια συστήματος

Στους Η/Υ αποθηκεύονται δεδομένα σε αρχεία που μπορεί να έχουν ιδιαίτερη αξία για τους χρήστες. Αρχεία τιμολογίων, εργασιών ή φωτογραφιών, είναι κάποια αρχεία που οι ιδιοκτήτες τους θα θέλουν να προστατεύσουν. Αρχεία και Η/Υ κινδυνεύουν από:

- Φυσικές καταστροφές
- Βλάβες υλικού
- Λάθος ή εσκεμμένους χειρισμούς χρηστών
- Από κακόβουλο λογισμικό (ιούς), κ.λπ.

Ο μόνος τρόπος για να προστατευτούν πλήρως τα σημαντικά αρχεία από τις παραπάνω απειλές είναι να βρίσκονται αποθηκευμένα σε αντίγραφο ασφαλείας.

Το ΛΣ παρέχει διάφορες επιλογές για να προστατευτούν τα αρχεία από κάποιες απειλές, οι βασικότερες από τις οποίες είναι:

1. **Αντίγραφα ασφαλείας (backup)**. Στα περισσότερα σύγχρονα ΛΣ υπάρχει βοηθητικό πρόγραμμα για λήψη Αντιγράφων Ασφαλείας των αρχείων που θέλει ο χρήστης, σε τακτά χρονικά διαστήματα.
2. **Κωδικός σύνδεσης (password)**. Συνοδεύει πάντα ένα *Όνομα Χρήστη* και δίνονται μαζί για να επιτραπεί η σύνδεση στον Η/Υ. Αποτελείται από γράμματα, αριθμούς και σύμβολα. Σ' αυτό, υπάρχει διάκριση μεταξύ πεζών και κεφαλαίων. Για μεγαλύτερη ασφάλεια προτείνεται: η χρήση τουλάχιστο 8 χαρακτήρων, να είναι φράση και όχι λέξη, να περιέχει συνδυασμό από γράμματα, αριθμούς και σύμβολα αν επιτρέπονται και να αλλάζουν σε τακτά χρονικά διαστήματα (πχ κάθε 3 μήνες).
3. **Έλεγχος πρόσβασης.** Ανάλογα με το σύστημα αρχείων, ο ιδιοκτήτης ενός αρχείου μπορεί να δώσει ή αφαιρέσει δικαιώματα πάνω σε αυτό (για χρήστες και ομάδες χρηστών).

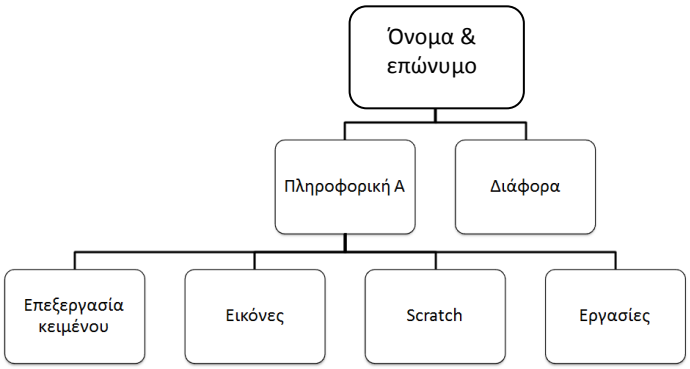
Το αντικείμενο της ασφάλειας συστήματος αναλύεται και παρουσιάζεται διεξοδικά στο Κεφάλαιο 5 αυτών των σημειώσεων

## Ερωτήσεις

1. Ποιες είναι οι διαφορές μεταξύ, κύριας μνήμης RAM και των βοηθητικών συσκευών μνήμης;
2. Τι είναι αρχείο ηλεκτρονικού υπολογιστή;
3. Τι είναι σύστημα αρχείων και πως οργανώνει τα αρχεία του;
4. Περιγράψτε τη διαδικασία Μορφοποίησης (Format) ενός σκληρού δίσκου.
5. Ποια είναι η χρησιμότητα των διαμερισμάτων (partitions) σ' ένα σκληρό δίσκο;
6. Για ποιους λόγους το σύστημα αρχείων NTFS είναι προτιμότερο από το FAT;
7. Ποιοι παράγοντες επηρεάζουν την ταχύτητα ενός σκληρού δίσκου;
8. Τι είναι ο κατακερματισμός και πως μπορεί να διορθωθεί;
9. Ποιοί τύποι αρχείων είναι γνωστότεροι και τι περιέχουν τα αρχεία αυτά;
10. Σε τι διαφέρει η Απόλυτη από τη Σχετική διαδρομή ενός αρχείου;
11. Τι θα συμβεί αν μετονομαστεί η επέκταση κάποιου αρχείου από .jpg σε .mp3;
12. Ποιες από τις παρακάτω εκφράσεις είναι σωστές:
    i. Με χρήση φακέλων μπορούν να οργανωθούν τα αρχεία ενός Η/Υ.
    ii. Μέσα σ' έναν φάκελο μπορούν να συνυπάρχουν υποφάκελοι και αρχεία.
    iii. Σ' έναν φάκελο επιτρέπεται να υπάρχουν δυο αρχεία με ακριβώς το ίδιο όνομα και επέκταση.

## Δραστηριότητες

1. Δημιουργείστε στον φάκελο *Έγγραφα:* ένα φάκελο με το όνομά σας και στη συνέχεια δημιουργήστε το δέντρο φακέλων όπως στην εικόνα.




2. Εντοπίστε τις βασικές Περιφερειακές Μονάδες αποθήκευσης του Υπολογιστή σας. Σε ποίο γράμμα αντιστοιχεί η κάθε μία από αυτές; Πως εμφανίζονται αυτές σε περιβάλλον Linux;

3. Αναζητήστε στις παρακάτω ιστοσελίδες γνωστές επεκτάσεις αρχείων:
   - http://www.file-extensions.org
   - http://en.wikipedia.org/wiki/List_of_file_formats
4. Κάνοντας δεξί κλικ πάνω στο όνομα ενός αρχείου εικόνας επιλέξτε Άνοιγμα με .. για να δείτε την εικόνα με διαφορετικό πρόγραμμα προβολής εικόνων.
5. Ανοίξτε το πρόγραμμα διαχείρισης αρχείων και αναζητήστε όλα τα αρχεία του φακέλου Έγγραφα. Ταξινομήστε τα ως προς: όνομα, μέγεθος, ημερομηνία τροποποίησης.
6. Εμφανίστε το σύστημα αρχείων που έχουν οι δευτερεύουσες συσκευές μνήμης του Η/Υ.
7. Αλλάξτε το όνομα του USB stick σας δίνοντας για νέο τα αρχικά γράμματα του ονοματεπώνυμού σας και τη χωρητικότητα που έχει η συσκευή (πχ SP-8gb).

# Κεφάλαιο 3

# Διεργασίες και Διαχείριση Κεντρικής Μνήμης

Σε ένα υπολογιστικό σύστημα η Κεντρική Μονάδα Επεξεργασίας (ΚΜΕ) εκτελεί τις εντολές που βρίσκονται στην κύρια μνήμη του. Οι εντολές αυτές ανήκουν σε προγράμματα τα οποία, όταν εκτελούνται, ονομάζονται διεργασίες. Λόγω της μεγάλης ταχύτητάς της η ΚΜΕ είναι δυνατό να εξυπηρετεί πολλές διεργασίες και να φαίνεται ότι αυτές εκτελούνται ταυτόχρονα. Ο τρόπος με τον οποίο η ΚΜΕ εξυπηρετεί πολλές διεργασίες μέσω του λειτουργικού συστήματος και ο τρόπος διαμοιρασμού της μνήμης για τις διεργασίες είναι **τα αντικείμενα** αυτού του κεφαλαίου.

### Διδακτικοί Στόχοι

Σε αυτό το κεφάλαιο θα μάθετε:

- Πώς η Κεντρική Μονάδα Επεξεργασίας εκτελεί περισσότερα του ενός προγράμματα.
- Ποια είναι η έννοια της διεργασίας, τα είδη των διεργασιών, τον κύκλο ζωής τους και τους τρόπους συγχρονισμού τους.
- Ποια είναι η κύρια και ποια η δευτερεύουσα μνήμη του υπολογιστή.
- Πώς η δευτερεύουσα μνήμη χρησιμοποιείται για ενίσχυση της κύριας.
- Ποια είναι τα μοντέλα διαχείρισης μνήμης που χρησιμοποιούνται.

### Διδακτικές Ενότητες

## 3.1 Εισαγωγή

Η κεντρική μονάδα επεξεργασίας (ΚΜΕ) και η κύρια μνήμη αποτελούν τα βασικά δομικά στοιχεία ενός υπολογιστικού συστήματος. Η πρώτη εκτελεί εντολές χειρισμού δεδομένων (λογικές και αριθμητικές πράξεις και μετακινήσεις) και η δεύτερη έχει αποθηκευμένες τις εντολές των προγραμμάτων που εκτελούνται καθώς και τα δεδομένα που γίνονται αντικείμενο διαχείρισης. Για να εκτελεστεί ένα πρόγραμμα θα πρέπει να έχει φορτωθεί στην κύρια μνήμη σε μορφή εντολών που μπορεί να εκτελέσει η ΚΜΕ και μετά να του παραχωρηθεί χρόνος στην ΚΜΕ.

Στην πιο απλή μορφή υπολογιστικού συστήματος που μπορεί να υπάρξει (π.χ συστήματα μικροελεγκτών) η εκτέλεση ενός προγράμματος αρχίζει με την τροφοδοσία του συστήματος με ρεύμα και τη φόρτωση του στη μνήμη. Συνεχίζει δε μέχρι το τέλος της τροφοδοσίας με ρεύμα ή το τέλος του προγράμματος. Εκτελούνται δε όλες οι εντολές που βρίσκονται στον αντίστοιχο χώρο εντολών στην μνήμη. Σε περίπτωση που ο μικροελεγκτής δεν έχει άλλες εντολές για εκτέλεση συνήθως εκτελεί συνεχόμενα την λεγόμενη εντολή μη λειτουργίας (No Operation, NOP) και ουσιαστικά βρίσκεται σε αδράνεια.

Στην περίπτωση ενός πιο σύνθετου υπολογιστικού συστήματος υπάρχει η δυνατότητα εκτέλεσης πολλών προγραμμάτων με τρόπο που φαίνεται ότι αυτά εκτελούνται ταυτόχρονα (concurrent). Με αυτή την δυνατότητα γίνεται εκμετάλλευση της ΚΜΕ σε πολύ μεγάλο βαθμό και ελαχιστοποιείται ο χρόνος που αυτή βρίσκεται σε αδράνεια.

Για αυτόν τον λόγο υπάρχει μια ομάδα προγραμμάτων που εκτελούνται συνεχώς και ανήκουν στον πυρήνα του λειτουργικού συστήματος. Μέρος των καθηκόντων τους είναι να «μοιράζουν» τον χρόνο της ΚΜΕ και τη διαθέσιμη μνήμη στα προγράμματα που φαίνονται ότι εκτελούνται ταυτόχρονα. Για παράδειγμα, όταν ένα πρόγραμμα που εκτελείται περιμένει δεδομένα από από τον πολύ πιο αργό (σε σχέση με την ΚΜΕ και την κύρια μνήμη) σκληρό δίσκο , τότε έχει τη δυνατότητα κάποιο άλλο πρόγραμμα να συνεχίσει την δική του εκτέλεση από το σημείο στο οποίο βρισκόταν.

Σε αυτό το κεφάλαιο θα γνωρίσουμε την έννοια της διεργασίας που αποτελεί βασικό στοιχείο για την πραγμάτωση της παραπάνω λειτουργίας και θα δούμε πώς με τη χρήση της έννοιας της διεργασίας και την κατάλληλη χρονοδρομολόγηση της ΚΜΕ και διαχείριση της κεντρικής μνήμης είναι δυνατή η αποτελεσματική λειτουργία του υπολογιστή.

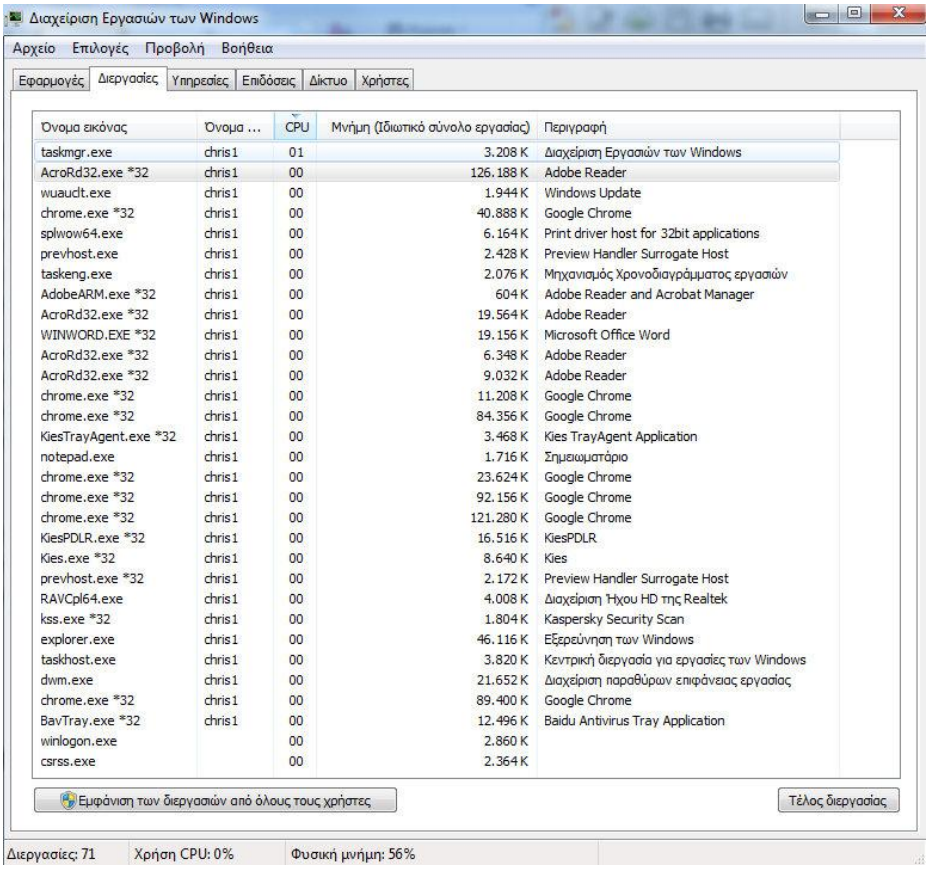
## 3.2 Διεργασίες

Με τον όρο *διεργασία* (process) νοείται ένα πρόγραμμα το οποίο έχει φορτωθεί στην κύρια μνήμη και βρίσκεται σε κατάσταση εκτέλεσης με αποτέλεσμα να καταναλώνει χρόνο της ΚΜΕ και πόρους του συστήματος (κύρια μνήμη, χώρο σε αποθηκευτικά μέσα, κανάλια επικοινωνίας). Η διεργασία δηλαδή εκφράζει κάτι δυναμικό και σε εξέλιξη σε αντίθεση με το πρόγραμμα που είναι κάτι στατικό.

Σε όλη τη διάρκεια της λειτουργίας του υπολογιστή γίνεται προσπάθεια η ΚΜΕ να είναι διαρκώς απασχολημένη με την εκτέλεση διεργασιών. Από την μεριά του χρήστη οι διεργασίες αυτές φαίνονται να είναι σε ταυτόχρονη εκτέλεση ενώ στην ουσία μόνο μια από όλες τις διεργασίες είναι σε εκτέλεση σε κάθε χρονική στιγμή σε ένα σύστημα με μια ΚΜΕ ενός πυρήνα. Αυτή η μέθοδος λειτουργίας ονομάζεται πολυπρογραμματισμός (multiprogramming)

και δίνει μια ψευδή εντύπωση παραλληλισμού. Θα πρέπει εδώ να αναφερθεί ότι για να υπάρχει πραγματική παράλληλη επεξεργασία θα πρέπει να υπάρχουν παραπάνω από ένας πυρήνες επεξεργασίας είτε μέσω ΚΜΕ πολλαπλών πυρήνων είτε μέσω πολλών ΚΜΕ είτε και τα δύο.

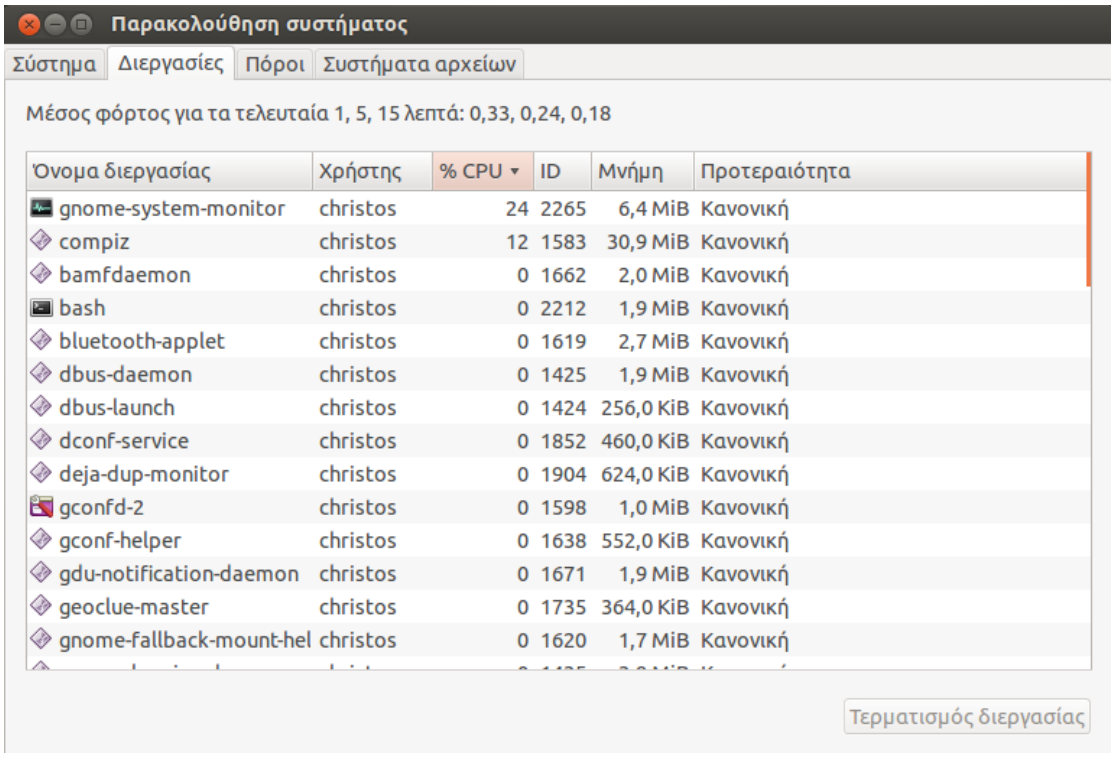
Μια εικόνα των διεργασιών που εκτελούνται στο σύστημα μας μπορούμε να έχουμε μέσω του προγράμματος Task Manager στα Windows το οποίο εμφανίζει τις διεργασίες όπως φαίνεται στην εικ. 3.1




Εικόνα 3.1: Οι διεργασίες σε έναν Η/Υ με ΛΣ Windows 7 όπως φαίνονται με την χρήση του προγράμματος Task Manager

Αντίστοιχη δυνατότητα σε λειτουργικά συστήματα βασιζόμενα στο UNIX έχουμε με χρήση της εντολής *gnome-system-monitor* (εικ. 3.2) για τη διανομή Ubuntu του λειτουργικού συστήματος Linux ή της εντολής ***ps*** (εικ. 3.3) σε περιβάλλον γραμμής εντολών (βλ. δραστηριότητες 7 και 8)

**3.2.1 Τα είδη των διεργασιών.** Οι διεργασίες μπορούν να αντιστοιχούν είτε σε διαφορετικά προγράμματα, είτε στο ίδιο πρόγραμμα όταν αυτό εκτελείται πολλές φορές ή μπορούν ακόμα να δημιουργούν με την σειρά τους νέες διεργασίες. Στην περίπτωση αυτή μιλάμε για τα *νήματα (threads)* και πρόκειται για τμήματα προγραμμάτων που μπορούν να εκτελεστούν «παράλληλα» μεταξύ τους.



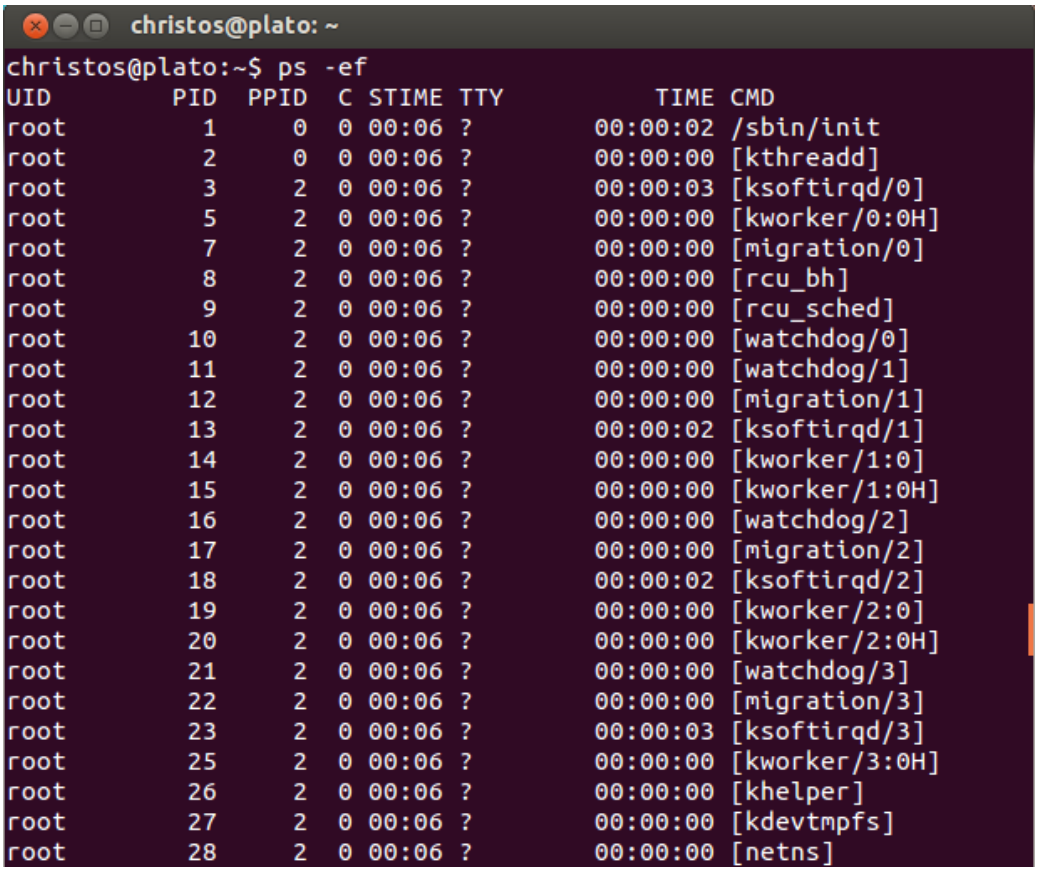

Εικόνα 3.2: Οι διεργασίες σε έναν Η/Υ με ΛΣ Ubuntu 12.04 όπως φαίνονται με την χρήση του προγράμματος gnome-system-monitor

**3.2.2 Καταστάσεις και κύκλος ζωής των διεργασιών.** Από τη δημιουργία μιας διεργασίας μέχρι την ολοκλήρωση και τον τερματισμό της υπάρχουν τρία *διακριτά* και επαναλαμβανόμενα στάδια. Έτσι, μια διεργασία μπορεί να είναι:

- *Εκτελούμενη (running):* Όταν απασχολεί την ΚΜΕ
- *Έτοιμη (runnable, ready):* Όταν, και αφού είχε σταματήσει προσωρινά να εκτελείται , είναι πλέον έτοιμη και περιμένει τη σειρά της για να πάρει χρόνο στην ΚΜΕ και να συνεχίσει την εκτέλεση της.
- *Υπό αναστολή (blocked):* Όταν περιμένει την ολοκλήρωση κάποιου εξωτερικού από αυτή συμβάντος (π.χ δεδομένα από κάποια περιφερειακή συσκευή) για να μπορεί να μεταβεί σε κατάσταση ετοιμότητας έτσι ώστε να μπορεί να εκτελεσθεί.

Κάθε φορά που μια διεργασία αλλάζει κατάσταση από εκτελούμενη στις δύο υπόλοιπες και αντίστροφα είναι απαραίτητη η λεγόμενη μεταγωγή περιβάλλοντος (context switching) όπου επαναφέρεται από ή αποθηκεύεται στη μνήμη όλη η αναγκαία για την εκτέλεση της διεργασίας διαμόρφωση (τιμές καταχωρητών, επόμενη εντολή προς εκτέλεση, περιεχόμενα κύριας μνήμης).

Η απόφαση για το ποια διεργασία θα περάσει από τη μία κατάσταση στην άλλη λαμβάνεται από τον *χρονοδρομολογητή διεργασιών* που είναι ένα πρόγραμμα του πυρήνα του λειτουργικού συστήματος. Η λειτουργία του στηρίζεται σε παραμέτρους που θα δούμε στην παράγραφο 3.2.4 παρακάτω.




Εικόνα 3.3: Οι διεργασίες σε έναν Η/Υ με ΛΣ Ubuntu 12.04 όπως φαίνονται με την χρήση του προγράμματος ps της γραμμής εντολών.

**3.2.3 Συγχρονισμός διεργασιών.** Κατά την διάρκεια εκτέλεσης των διεργασιών πολλές από αυτές είναι δυνατόν να θελήσουν να κάνουν κοινή χρήση περιφερειακών συσκευών και κοινών πόρων του συστήματος. Αυτό το γεγονός δημιουργεί *συνθήκες ανταγωνισμού* και θα μπορούσε να οδηγήσει από το αμοιβαίο μπλοκάρισμα των διεργασιών (όπου δυο ή παραπάνω διεργασίες μπλοκάρουν αμοιβαία η μία την άλλη), μέχρι την προβληματική λειτουργία τους (π.χ αλλαγή των δεδομένων μιας διεργασίας από μια άλλη)

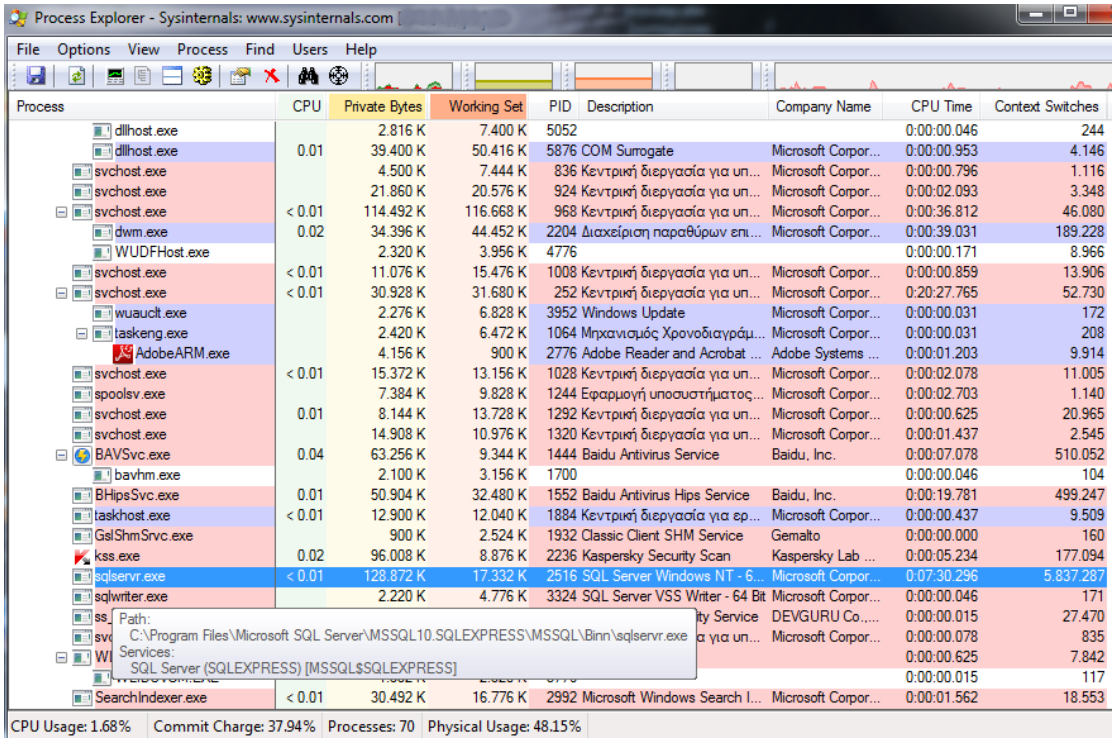
Μια σημαντική έννοια στο θέμα του συγχρονισμού των διεργασιών είναι αυτή του *κρίσιμου τμήματος* (critical section). Κάθε φορά που μια διεργασία εισέρχεται σε τμήμα του προγράμματος που εκτελείται και έχει πρόσβαση σε διαμοιραζόμενους πόρους λέμε ότι βρίσκεται στο κρίσιμο τμήμα της. Δημιουργείται έτσι επίσης η έννοια του *αμοιβαίου αποκλεισμού* που συνιστά την απαγόρευση μιας διεργασίας να εισέρθει στο κρίσιμο τμήμα της όταν μια άλλη βρίσκεται στο αντίστοιχο δικό της.

Για τον λόγο αυτό υπάρχει μηχανισμός επικοινωνίας μεταξύ των διεργασιών (Inter Process Communication, IPC) ο οποίος υλοποιείται με διάφορες μεθόδους (αρχεία, κανάλια επικοινωνίας, ροές δεδομένων, σήματα, σηματοφορείς, ουρές μηνυμάτων κ.ά).

**3.2.4 Χρονοδρομολόγηση διεργασιών.** Η χρονοδρομολόγηση των διεργασιών έχει ουσιαστικά να κάνει με την χρονοδρομολόγηση της ΚΜΕ και όπως έχει ήδη αναφερθεί γίνεται από τον χρονοδρομολογητή (scheduler).

Η χρονοδρομολόγηση λαμβάνει χώρα σε δυο επίπεδα:

- *Μακροχρόνια χρονοδρομολόγηση (long term scheduling ή job scheduling).* Εδώ καθορίζεται ποιες από τις διεργασίες που έχουν υποβληθεί από τους χρήστες για εκτέλεση θα φορτωθούν στην μνήμη και θα γίνουν έτοιμες για εκτέλεση.
- *Βραχυχρόνια χρονοδρομολόγηση (short term ή CPU scheduling).* Εδώ επιλέγονται οι διεργασίες από την λίστα έτοιμων διεργασιών που θα τους παραχωρηθεί χρόνος στην ΚΜΕ έτσι ώστε να γίνουν εκτελούμενες.




Εικόνα 3.4: Απεικόνιση διεργασιών σε υπολογιστή με ΛΣ Windows 7 με χρήση του προγράμματος process explorer (διαθέσιμο και για Linux). Η τελευταία δεξιά στήλη αναφέρεται στο πλήθος των μεταγωγών περιβάλλοντος.

Ο χρονοδρομολογητής αποφασίζει για το πότε και ποια διεργασία θα διακοπεί και ποια θα συνεχίσει με βάση κάποια κριτήρια. Τα πιο συνηθισμένα από τα οποία βασίζονται στις εξής έννοιες:

- *Αποδοτικότητα (efficiency)*: Η ΚΜΕ θα πρέπει να είναι απασχολημένη κατά το μεγαλύτερο δυνατό χρονικό διάστημα.
- *Δικαιοσύνη (fairness)*: Ο χρόνος της ΚΜΕ θα πρέπει να μοιράζεται δίκαια μεταξύ των έτοιμων προς εκτέλεση διεργασιών.
- *Χαμηλό χρόνο απόκρισης (low response time)*: Ο χρόνος αναμονής μέχρι την πρώτη έξοδο-απόκριση σε ένα διαλογικό σύστημα πρέπει να είναι χαμηλός.
- *Χαμηλό χρόνο διεκπεραίωσης (low turnaround time).* Ο συνολικός χρόνος για την πλήρη εκτέλεση μιας εργασίας πρέπει να είναι χαμηλός.

Ανάλογα με τη στρατηγική που ακολουθούν οι αλγόριθμοι χρονοδρομολόγησης διακρίνονται σε δύο κατηγορίες:

- *Μη διακοπτοί (non preemptive) αλγόριθμοι:* Μια διεργασία που έχει τον έλεγχο της ΚΜΕ τον διατηρεί μέχρις ότου ολοκληρωθεί ή χρειαστεί κάποια άλλη λειτουργία.
- *Διακοπτοί (preemptive) αλγόριθμοι:* Ο χρόνος της ΚΜΕ μοιράζεται σε χρονικά διαστήματα όμοια ή διαφορετικά μεταξύ τους (κβάντα χρόνου) και αυτά μοιράζονται στις διεργασίες με σειρά η οποία καθορίζεται είτε από τη στιγμή άφιξης της διεργασίες είτε από τον απαιτούμενο χρόνο εκτέλεσης της.

Εργαζόμενοι με βάση τα παραπάνω οι αλγόριθμοι χρονοδρομολόγησης καθορίζουν τη σειρά και τον χρόνο εκτέλεσης των διεργασιών. Σε πολλές περιπτώσεις αυτή η σειρά μπορεί να τροποποιηθεί με βάση κάποια προτεραιότητα που ορίζεται από τον χρήστη για κάποιες διεργασίες μέσω των προγραμμάτων διαχείρισης διεργασιών.

## 3.3 Διαχείριση Μνήμης

Οι διεργασίες που είδαμε ότι μπορούν να συνυπάρχουν σε κάθε χρονική στιγμή έχουν ανάγκη από την κύρια μνήμη του υπολογιστή. Με τον όρο *κύρια μνήμη* του υπολογιστή αναφερόμαστε στην μνήμη η οποία δεν διατηρεί τα περιεχόμενα της όταν σταματάει η λειτουργία του υπολογιστή και παρέχει ταχύτατη και άμεση προσπέλαση σε οποιαδήποτε θέση της για ανάγνωση ή για εγγραφή. Αν και ο ορισμός αυτός αναφέρεται στην RAM (Random Access Memory, μνήμη τυχαίας προσπέλασης), εντούτοις στην κύρια μνήμη συμπεριλαμβάνεται συμπληρωματικά και η μνήμη ROM (Read Only Memory, μνήμη εγγραφής μόνο) στην οποία υπάρχουν μόνιμα εγγεγραμμένα βασικά προγράμματα διαχείρισης του υλικού από τον κατασκευαστή του.

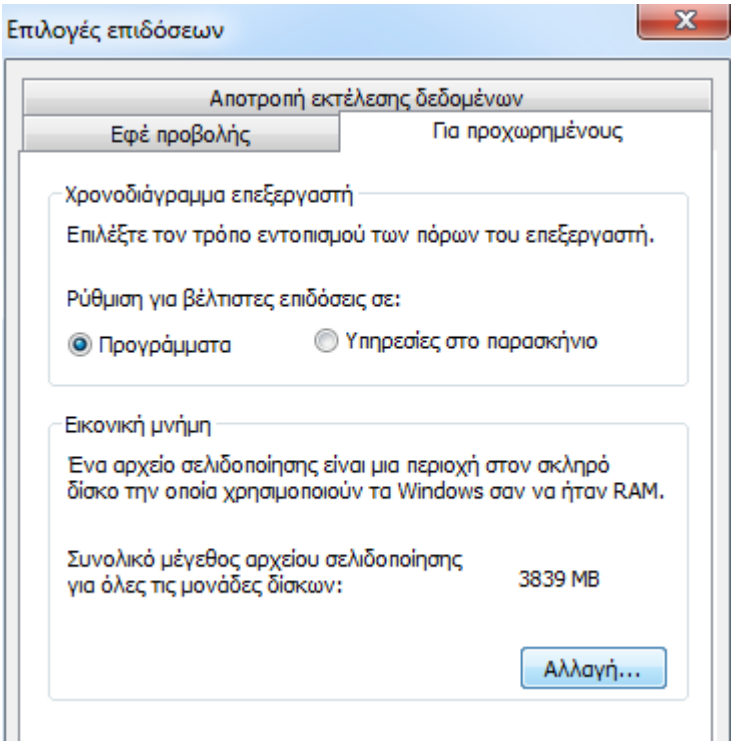
Σε έναν υπολογιστή βέβαια, εκτός από την κύρια μνήμη, υπάρχει και η *δευτερεύουσα μνήμη* (σκληροί δίσκοι, CD/DVD, δισκέτες, μνήμες flash), με χαρακτηριστικό της γνώρισμα την διατήρηση των περιεχομένων της ακόμα και χωρίς να λειτουργεί ο υπολογιστής και την αρκετά μικρότερη ταχύτητα πρόσβασης σε σχέση με την κύρια.

Έχοντας λοιπόν στη διάθεση του την κύρια και την δευτερεύουσα μνήμη το Λειτουργικό Σύστημα θα πρέπει να κάνει την καλύτερη δυνατή διαχείριση τους έτσι ώστε να εξυπηρετηθούν όσο το δυνατόν περισσότερες διεργασίες. Θα πρέπει εδώ να πούμε ότι αναφερόμαστε επίσης και στην δευτερεύουσα μνήμη σε αυτή την ενότητα καθώς, όπως θα δούμε παρακάτω, είναι δυνατή η χρήση ενός μέρους της προκειμένου να αυξηθεί η διαθέσιμη στις διεργασίες ποσότητα μνήμης μέσω της ανταλλαγής (swapping) και της εικονικής μνήμης (virtual memory). Στη συνέχεια με τον όρο μνήμη θα αναφερόμαστε γενικά στη διαθέσιμη στις διεργασίες μνήμη.

**3.3.1 Κατανομή της μνήμης στις διεργασίες.** Η κατανομή της μνήμης στις διεργασίες γίνεται από το Λειτουργικό Σύστημα *και είναι είτε στατική είτε δυναμική.*

Στην *στατική* κατανομή η μνήμη είναι χωρισμένη εκ των προτέρων σε τμήματα τα οποία είναι διαφόρων μεγεθών και διατίθενται στις διεργασίες ανάλογα με τις ανάγκες τους. Είναι ο απλούστερος τρόπος κατανομής μνήμης αλλά τα τμήματα μνήμης δεν αξιοποιούνται πλήρως και δεν είναι εύκολα δυνατή η από κοινού χρήση τους από συσχετιζόμενες διεργασίες.

Στη *δυναμική* κατανομή το Λειτουργικό Σύστημα παρέχει στις διεργασίες όση μνήμη απαιτούν όταν αρχίσουν να εκτελούνται. Λύνει βασικά προβλήματα αξιοποίησης της μνήμης αλλά απαιτεί πιο σύνθετες και πολύπλοκες διαδικασίες για την διάθεση και τον έλεγχο της μνήμης.




Εικόνα 3.5: Ορισμός της εικονικής μνήμης σε σύστημα Windows 7

Όταν η κύρια μνήμη η οποία είναι ταχύτερη αλλά λιγότερη από την δευτερεύουσα δεν επαρκεί για το πλήθος των διεργασιών, τότε το Λειτουργικό Σύστημα έχει τη δυνατότητα της *ανταλλαγής* (swapping). *Σε αυτή την περίπτωση μεταφέρονται προσωρινά* στη δευτερεύουσα μνήμη περιοχές της κύριας που δεν είναι απαραίτητο να βρίσκονται στην κύρια μνήμη. Όταν τα περιεχόμενα τους απαιτηθούν τότε μεταφέρονται και πάλι οι περιοχές αυτές στην κύρια μνήμη και αντίστοιχα μεταφέρονται άλλες από την κύρια στην δευτερεύουσα.

**3.3.2 Εικονική μνήμη.** Όπως αναφέρθηκε και παραπάνω υπάρχει δυνατότητα συνεργασίας της κύριας με την δευτερεύουσα μνήμη προκειμένου η συνολικά διαθέσιμη μνήμη στις διεργασίες να είναι μεγαλύτερη της φυσικής μνήμης. Η δυνατότητα αυτή αναφέρεται γενικά ως *εικονική μνήμη (virtual memory)* και επιτρέπει στους προγραμματιστές να γράφουν προγράμματα χωρίς να τους απασχολεί απαραίτητα η φυσική μνήμη του συστήματος στο οποίο θα εκτελεστούν. Οι διευθύνσεις μνήμης που χρησιμοποιούνται από τα προγράμματα είναι εικονικές και μετατρέπονται σε πραγματικές κατά τη στιγμή της εκτέλεσης τους με βάση την θέση της μνήμης στην οποία φορτώθηκε αρχικά το πρόγραμμα για να εκτελεστεί. Το μέγεθος της εικονικής μνήμης προσδιορίζεται συνήθως στο 150% της φυσικής μνήμης, δηλαδή για ένα σύστημα με 4GB RAM η εικονική μνήμη θα ορισθεί στα 6GB περίπου.

**3.3.3 Σελιδοποίηση και κατάτμηση.** Η μετατροπή και η αντιστοίχιση των εικονικών διευθύνσεων μνήμης στις αντίστοιχες φυσικές διευθύνσεις για τη χρήση τους από τις διεργασίες γίνεται με διάφορους τρόπους. Η σελιδοποίηση και η κατάτμηση είναι οι δύο βασικές στρατηγικές που χρησιμοποιούνται.

***Σελιδοποίηση (paging).*** Με τη στρατηγική της σελιδοποίησης η εικονική μνήμη (κύρια + μέρος της δευτερεύουσας) χωρίζεται σε ισομεγέθεις σελίδες και η φυσική μνήμη (κύρια) χωρίζεται

σε αντίστοιχες ενότητες του ίδιου μεγέθους. Προφανώς το πλήθος των σελίδων της εικονικής μνήμης είναι πάντα μεγαλύτερο από αυτό των ενοτήτων.

Οι διευθύνσεις που χειρίζονται οι διεργασίες είναι εικονικές διευθύνσεις (ΕΔ). Για την αντιστοίχισή τους σε φυσικές διευθύνσεις (ΦΔ) είναι απαραίτητη μια διαδικασία κατά την οποία γίνεται χρήση ενός πίνακα αντιστοίχισης σελίδων – ενοτήτων.

Σε περίπτωση που απαιτηθεί πρόσβαση σε σελίδα που δεν αντιστοιχεί σε ενότητα που βρίσκεται στην φυσική μνήμη τότε πρέπει να πραγματοποιηθεί μια διαδικασία μεταφοράς της σελίδας αυτής από την δευτερεύουσα στην φυσική μνήμη. Ταυτόχρονα θα πρέπει να γίνει απελευθέρωση κάποιας ενότητας από την φυσική μνήμη και μεταφορά της στην δευτερεύουσα μνήμη.

Ένα μειονέκτημα της σελιδοποίησης είναι ότι η τελευταία σελίδα που χρησιμοποιείται από κάποια διεργασία δεν χρησιμοποιείται πλήρως. Αυτό ονομάζεται *εσωτερικός κατακερματισμός (internal fragmentation).*

***Κατάτμηση (segmentation).*** Με την τεχνική της κατάτμησης γίνεται μια προσπάθεια αποφυγής του εσωτερικού κατακερματισμού. Αποδίδεται ετσι σε κάθε διεργασία όση μνήμη απαιτείται και η μνήμη χωρίζεται σε τμήματα διαφορετικού μεγέθους. Η αντιστοίχιση των εικονικών διευθύνσεων σε φυσικές γίνεται και πάλι με την βοήθεια ενός πίνακα αντιστοίχισης όπου για κάθε τμήμα διατηρούνται η αρχική του διεύθυνση στη μνήμη και το μέγεθος του. Αν χρειαστεί ανταλλαγή και μεταφορά από την δευτερεύουσα στην κύρια μνήμη, τότε πραγματοποιούνται με τον ίδιο τρόπο όπως και στην σελιδοποίηση.

Μια διεργασία μπορεί να χρησιμοποιεί παραπάνω από ένα τμήματα διαφορετικού μεγέθους. Σε περίπτωση που η διεργασία ή κάποιο από τα τμήματα της παύσει να είναι απαραίτητο να υπάρχει τότε δημιουργείται ένα κενό στον αντίστοιχο χώρο που καταλάμβανε. Αυτό ονομάζεται *εξωτερικός κατακερματισμός* και η αντιμετώπιση του γίνεται με τον συνδυασμό των μεθόδων της σελιδοποίησης και της κατάτμησης κατά τις οποίες τα τμήματα της κατάτμησης είναι διαφορετικά μεταξύ τους και πάλι αλλά αποτελούνται από ισομεγέθεις σελίδες. Για την αντιμετώπιση της εξωτερικής κατάτμησης είναι δυνατό να εκτελεστεί ένας αλγόριθμος «ανασυγκρότησης» της μνήμης κατά τα πρότυπα της ανασυγκρότησης δίσκων από το Λειτουργικό Σύστημα αλλά αυτό θα ήταν αρκετά χρονοβόρο.

## Ερωτήσεις

1. Ποιος είναι ο κύριος ρόλος της ΚΜΕ και της μνήμης;
2. Με ποιο τρόπο αυξάνεται ο βαθμός εκμετάλλευσης της ΚΜΕ;
3. Για ποιό λόγο μπορεί κάποιο πρόγραμμα που εκτελείται να αναγκαστεί να περιμένει;
4. Τι εννοούμε με τον όρο διεργασία; Σε τι διαφέρει από το πρόγραμμα;
5. Τι ονομάζεται πολυπρογραμματισμός;
6. Πώς μπορεί να επιτευχθεί πραγματική παράλληλη επεξεργασία;
7. Πόσα είδη διεργασιών υπάρχουν;
8. Σε ποιες καταστάσεις μπορεί να βρίσκεται μια διεργασία;
9. Τι συμβαίνει στη μεταγωγή περιβάλλοντος;
10. Ποιος είναι ο ρόλος του χρονοδρομολογητή διεργασιών;
11. Πότε μπορούν να υπάρξουν συνθήκες ανταγωνισμού μεταξύ των διεργασιών; Γιατί πρέπει να υπάρχει συγχρονισμός μεταξύ τους;
12. Τι συμβαίνει όταν μια διεργασία εισέρχεται στο κρίσιμο τμήμα της;
13. Σε πόσα επίπεδα συμβαίνει η χρονοδρομολόγηση της ΚΜΕ;

14. Ποια είναι τα συνηθισμένα κριτήρια χρονοδρομολόγησης;
15. Σε ποιες κατηγορίες χωρίζονται οι χρονοδρομολογητές; Ποιο είναι το χαρακτηριστικό καθεμίας;
16. Σε τι διαφέρει η κύρια από την δευτερεύουσα μνήμη;
17. Σε τι διαφέρει η στατική από την δυναμική κατανομή μνήμης;
18. Τι συμβαίνει κατά την ανταλλαγή μνήμης;
19. Ποια δυνατότητα ονομάζεται εικονική μνήμη και τι συμβαίνει με τις διευθύνσεις μνήμης των προγραμμάτων;
20. Πως λειτουργεί η σελιδοποίηση;
21. Τι συμβαίνει όταν μια σελίδα της εικονικής μνήμης δεν αντιστοιχεί σε ενότητα της φυσικής;
22. Τι ονομάζεται εσωτερικός κατακερματισμός;
23. Πως λειτουργεί η κατάτμηση;
24. Τι ονομάζεται εξωτερικός κατακερματισμός και πώς γίνεται η αντιμετώπιση του;

## Δραστηριότητες

**Windows**

1. Σε έναν υπολογιστή με ΛΣ Windows XP ή Windows 7 πατήστε ταυτόχρονα Ctrl+Alt+Del για να εκκινήσετε τον διαχειριστή διεργασιών (Task Manager) όπως φαίνεται στην εικ. 3.1. Εξετάστε τις πληροφορίες που σας παρέχει και δοκιμάστε να τερματίσετε κάποια διεργασία.
2. Από τον διαχειριστή διεργασιών αλλάξτε την προτεραιότητα κάποιων διεργασιών.
3. Εκτελώντας το πρόγραμμα *msconfig* των Windows εξετάστε τα στοιχεία που κάνουν εκκίνηση κατά την έναρξη λειτουργίας του Η/Υ
4. Από τον διαχειριστή διεργασιών και από την καρτέλα *επιδόσεις* επιλέξτε την *εποπτεία πόρων* για να δείτε την λεπτομερή ανάθεση μνήμης στις διεργασίες.
5. Ελέγξτε και ρυθμίστε την ποσότητα εικονικής μνήμης του υπολογιστή σας μέσω του *Πίνακα Ελέγχου > Σύστημα > Ρυθμίσεις Συστήματος για Προχωρημένους > Για προχωρημένους > Επιδόσεις > Για προχωρημένους (βλέπε εικ. 3.5).*
6. Εγκαταστήστε το πρόγραμμα process explorer από τη διεύθυνση https://technet.microsoft.com/en-us/sysinternals/bb896653 και ελέγξτε τις πληροφορίες που σας παρέχει για κάθε διεργασία.
7. Ανοίξτε ένα παράθυρο του Windows Explorer κάνοντας διπλό κλικ στον «Υπολογιστή μου» και ελέγξτε τα περιεχόμενα του δίσκου C:, αφού έχετε ορίσει πρώτα να εμφανίζονται τα κρυφά αρχεία και τα αρχεία συστήματος. Συγκρίνετε το μέγεθος του αρχείου pagefile.sys με το μέγεθος του αρχείου σελιδοποίησης για την εικονική μνήμη που αντιστοιχεί στον δίσκο C:. Τι παρατηρείτε;

**Linux (ubuntu)**

8. Ανοίξτε ένα τερματικό και πληκτρολογήστε την εντολή *ps*. Παρατηρήστε την έξοδο της. Για εξήγηση της λειτουργίας της και περισσότερες παραμέτρους πληκτρολογήστε την εντολή *man ps*.
9. Ανοίξτε ένα τερματικό και πληκτρολογήστε την εντολή *gnome-system-monitor*. Ελέγξτε τις δυνατότητες που σας δίνει αυτή η εφαρμογή μέσω του γραφικού της περιβάλλοντος.

# Κεφάλαιο 4.

## Διαχείριση Συσκευών Ε/Ε

Ένα υπολογιστικό σύστημα εκτός από την ΚΜΕ και την κύρια μνήμη που χρησιμοποιούνται για την επεξεργασία και προσωρινή αποθήκευση δεδομένων βασίζεται στις περιφερειακές συσκευές για την επικοινωνία με τον εξωτερικό κόσμο και για την βοηθητική (δευτερεύουσα) μνήμη. Η χρήση των περιφερειακών συσκευών επιτυγχάνεται λόγω της σχεδίασης του συστήματος και της ύπαρξης κατάλληλου υλικού και λογισμικού.

### Διδακτικοί Στόχοι

Σε αυτό το κεφάλαιο θα μάθετε:

- Για την αναγκαιότητα,
- τον τρόπο συνεργασίας,
- τις δυνατότητες και
- τον τρόπο εγκατάστασης των περιφερειακών συσκευών.

### Διδακτικές Ενότητες

4.1 Εισαγωγή

4.2 Είσοδος-έξοδος και περιφερειακές συσκευές

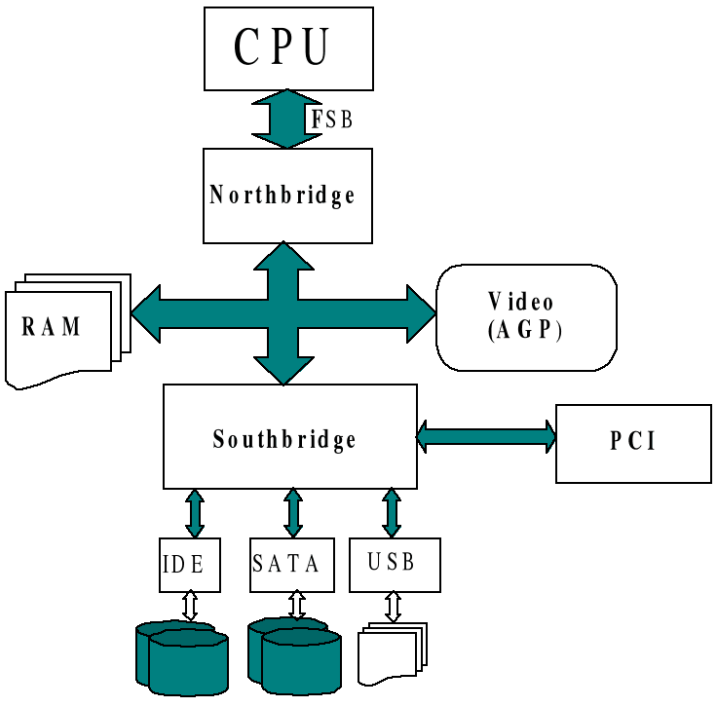
4.3 Ελεγκτές και οδηγοί συσκευών Ε/Ε.

4.4 Διαχείριση των περιφερειακών συσκευών από το Λειτουργικό Σύστημα.

## 4.1 Εισαγωγή

Όπως είναι γνωστό, ένα υπολογιστικό σύστημα αποτελείται από επιμέρους υποσυστήματα τα οποία διασυνδέονται μεταξύ τους για να ανταλλάσουν δεδομένα. Έχοντας μια γενική σχεδίαση, όπως αυτή που φαίνεται στην εικ. 4.1, η Κεντρική Μονάδα Επεξεργασίας (ΚΜΕ, CPU) επικοινωνεί με τη μνήμη RAM και τις περιφερειακές μονάδες μέσω ενός συστήματος διαδρόμων (bus) που μεταφέρουν δεδομένα και σήματα ελέγχου. Σε ένα υπολογιστικό σύστημα υπάρχουν διαφορετικές κατηγορίες διαδρόμων ανάλογα με την ταχύτητα επικοινωνίας και τον τύπο των υποσυστημάτων που διασυνδέουν.

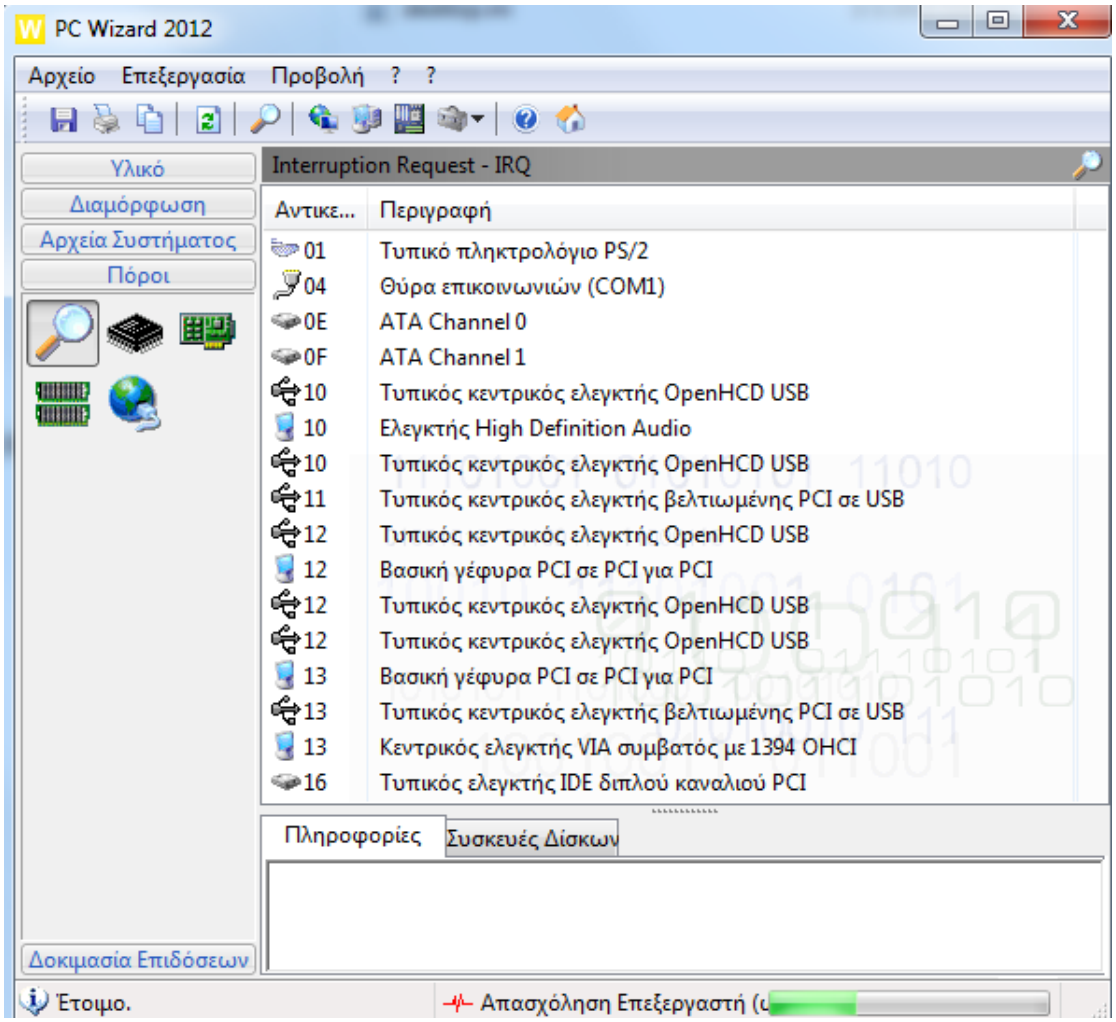
Αυτές είναι α) οι διάδρομοι μνήμης-επεξεργαστή, β) οι διάδρομοι εισόδου-εξόδου και γ) οι επίπεδοι (flat ή backplane) διάδρομοι.




Εικόνα 4.1: Διασύνδεση μονάδων ενός υπολογιστή με βάση το μοντέλο βόρειας και νότιας γέφυρας (northbridge, southbridge). Τα πράσινα βέλη δηλώνουν τους διαδρόμους επικοινωνίας (bus). Το FSB (Front Side Bus) είναι ο διάδρομος επικοινωνίας της ΚΜΕ με την βόρεια γέφυρα (*πηγή: Wikipedia)*

Οι τρεις αυτές κατηγορίες διαδρόμων υπάρχουν σε όλες τις σύγχρονες υπολογιστικές μονάδες, μαζί με σχεδιαστικές βελτιώσεις και διαφοροποιήσεις τους, με στόχο την επίτευξη ταχύτερης επικοινωνίας. Έτσι, βλέπουμε στα σημερινά συστήματα την ύπαρξη δυο κυκλωμάτων υποστήριξης της επικοινωνίας, την Βόρεια Γέφυρα (North Bridge) και τη Νότια Γέφυρα (South Bridge). Η *Βόρεια Γέφυρα* είναι αυτή που είναι υπεύθυνη για την επικοινωνία μεταξύ του επεξεργαστή, της μνήμης και του συστήματος γραφικών ενώ *η Νότια Γέφυρα* έχει αναλάβει την επικοινωνία μεταξύ όλων των άλλων πιο αργών συστημάτων.

Βασικό στοιχείο στην επικοινωνία μεταξύ των υποσυστημάτων σε έναν υπολογιστή είναι το *πρωτόκολλο επικοινωνίας διαδρόμου* δηλαδή το σύνολο των κανόνων που καθορίζουν το πώς γίνεται η επικοινωνία. Οι κανόνες αυτοί ρυθμίζουν ποιες είναι οι διαδικασίες και η μορφή των σημάτων ελέγχου και δεδομένων. Ένα σημαντικό στοιχείο επίσης είναι οι *διακοπές*, δηλαδή σήματα για αιτήματα επικοινωνίας. Αυτές χωρίζονται σε *διακοπές υλικού* και *διακοπές λογισμικού*. Ουσιαστικά οι διακοπές είναι ο τρόπος με τον οποίο μια συσκευή, ένα πρόγραμμα ή το Λειτουργικό Σύστημα αποκρίνεται σε αιτήματα επικοινωνίας ή «ζητάει την προσοχή» (δηλαδή χρόνο στον επεξεργαστή).




Εικόνα 4.2: Η κατανομή των διακοπών υλικού όπως προβάλλεται από το πρόγραμμα PC Wizard.

Βασιζόμενη στην παραπάνω σχεδίαση που αναφέρθηκε περιληπτικά, είναι δυνατή η σύνδεση περιφερειακών συσκευών σε μια υπολογιστική μονάδα η οποία είναι αναγκαία αφενός για την επικοινωνία του υπολογιστικού συστήματος με τον χρήστη και με άλλα υπολογιστικά συστήματα, αφετέρου για τον εμπλουτισμό του συστήματος με νέες δυνατότητες κυρίως όσον αφορά στα μέσα δευτερεύουσας μνήμης. Στο κεφάλαιο αυτό θα γνωρίσουμε τα είδη των περιφερειακών συσκευών που μπορούν να συνδεθούν καθώς και τα απαιτούμενα στοιχεία για τη σωστή διασύνδεση τους.

## 4.2 Είσοδος – Έξοδος και Περιφερειακές Συσκευές

Οι περιφερειακές συσκευές σε έναν υπολογιστή μπορεί να είναι συσκευές δευτερεύουσας μνήμης (σκληροί δίσκοι, CD/DVD, Flash disks) ή συσκευές εισόδου-εξόδου για την επικοινωνία με τον χρήστη ή με άλλα υπολογιστικά συστήματα.

***Συσκευές δευτερεύουσας μνήμης***

Με τον όρο αυτό αναφερόμαστε σε συσκευές αποθήκευσης δεδομένων όπως οι σκληροί δίσκοι και οι συσκευές ανάγνωσης οπτικών δίσκων (CD/DVD/Blue Ray). Για τους σκληρούς δίσκους η συνεχής εξέλιξη έχει οδηγήσει στην ύπαρξη τόσο μαγνητικών σκληρών δίσκων (Hard Disk Drives) όσο και συσκευών μόνιμης αποθήκευσης σε ολοκληρωμένα κυκλώματα μνήμης (flash disks ή Solid State Drives) που όμως ακολουθούν τις ίδιες αρχές όσον αφορά στην οργάνωση του μέσου αποθήκευσης (τομείς, τροχιές, ενότητες κτλ). Η επικοινωνία αυτών των συσκευών με τον επεξεργαστή και την κύρια μνήμη του υπολογιστή γίνεται με χρήση διαφόρων τύπων σύνδεσης. Η σύνδεση USB είναι αυτή την περίοδο η κύρια μέθοδος για αποσπώμενες συσκευές και η SATA για τις ενσωματωμένες στον υπολογιστή συσκευές. Μέσα αποθήκευσης όπως οι μαγνητικές ταινίες και οι δισκέτες (floppy disks) καθώς και οι αντίστοιχες συσκευές ανάγνωσης και εγγραφής σε αυτές έχουν αρχίσει να εκλείπουν εδώ και αρκετά χρόνια.

Σε ένα σύγχρονο υπολογιστικό σύστημα (2015) θα δούμε μέγεθος κύριας μνήμης (RAM) από 2 μέχρι 4 Gigabytes συνήθως να συνδυάζεται με μέγεθος δευτερεύουσας μνήμης της τάξης των 500 με 1000 Gigabytes (1 Terabyte) όσον αφορά τους μαγνητικούς σκληρούς δίσκους. Η δε χρήση μνήμης flash είναι της τάξης των 16-32 Gigabyte καθώς είναι μεν πιο γρήγορη, όμως είναι και αρκετά πιο ακριβή.

Η χρήση των συσκευών δευτερεύουσας μνήμης και κυρίως των ενσωματωμένων σκληρών δίσκων είναι σημαντική για τη δυνατότητα εικονικής μνήμης που αναφέρθηκε στο κεφάλαιο 3. Όπως αναφέρθηκε εκεί, το συνηθισμένο μέγεθος της εικονικής μνήμης είναι περίπου μιάμιση φορά την πραγματική. Δηλαδή για 4 Gbyte RAM θα καθορίσουμε και 6 Gigabyte εικονικής μνήμης στον σκληρό δίσκο.

***Συσκευές εισόδου/εξόδου***

Οι συσκευές εισόδου/εξόδου είναι συσκευές διεπαφής (επικοινωνίας) με τον χρήστη και διακρίνονται σε συσκευές *εισόδου* δεδομένων όπως το πληκτρολόγιο, το ποντίκι, το μικρόφωνο, ο σαρωτής (scanner) και συσκευές *εξόδου* όπως η οθόνη, τα ηχεία, ο εκτυπωτής, ο σχεδιαστής (plotter) κ.α. Υπάρχουν δε και συσκευές που είναι ταυτόχρονα εισόδου και εξόδου και είναι οι οθόνες αφής (touch screens) που είναι αρκετά διαδεδομένες στα σύγχρονα κινητά τηλέφωνα (smartphones) και υπολογιστές ταμπλέτες (tablets) και επίσης και τα *hands free* μέσω καλωδίων ή Bluetooth.

Στις συσκευές επικοινωνίας συμπεριλαμβάνονται επίσης και οι συσκευές δικτύωσης μέσω τεχνολογίας ενσύρματων ή ασύρματων τοπικών δικτύων (LAN ή WiFi), μέσω Bluetooth ή δικτύων κινητής τηλεφωνίας.

### 4.3 Ελεγκτές και Οδηγοί Συσκευών Ε/Ε

Για να είναι δυνατή η σύνδεση της συσκευής στο υπολογιστικό σύστημα και η επιτυχής λειτουργία της είναι απαραίτητο να υπάρχουν ένα κύκλωμα προσαρμογής και ελέγχου της συσκευής, ο *ελεγκτής (controller),* και ένα πρόγραμμα που αναλαμβάνει την επικοινωνία με το Λειτουργικό Σύστημα, ο *οδηγός (driver).* Το πρόγραμμα αυτό σε συνεργασία με το αντίστοιχο

υλικό αναλαμβάνει την επικοινωνία με το υπόλοιπο σύστημα χρησιμοποιώντας μεταξύ άλλων τις *διακοπές* (υλικού και λογισμικού) και τα κανάλια DMA (Direct Memory Access).

Λόγω της εξέλιξης της τεχνολογίας τα κυκλώματα ελέγχου είναι πολλές φορές ενσωματωμένα στη συσκευή (π.χ σκληροί δίσκοι) και η επικοινωνία, όσον αφορά στο υλικό μέρος, γίνεται μέσω τυποποιημένων κυκλωμάτων και πρωτόκολλων διαδρόμων και θυρών επικοινωνίας (π.χ IDE, SATA, USB, PS2, RS232, PCI, AGP κ.ά).

Επίσης, λόγω της εξέλιξης στην τεχνολογία λογισμικού και των λειτουργικών συστημάτων, πολλές φορές τα προγράμματα οδήγησης της συσκευής (οδηγοί) είναι ήδη ενσωματωμένα στο Λειτουργικό Σύστημα ή μπορούν να βρεθούν με αυτόματη διαδικασία αναζήτησης στο διαδίκτυο σε αποθετήρια (repositories) λογισμικού της εταιρείας κατασκευής του λειτουργικού συστήματος.

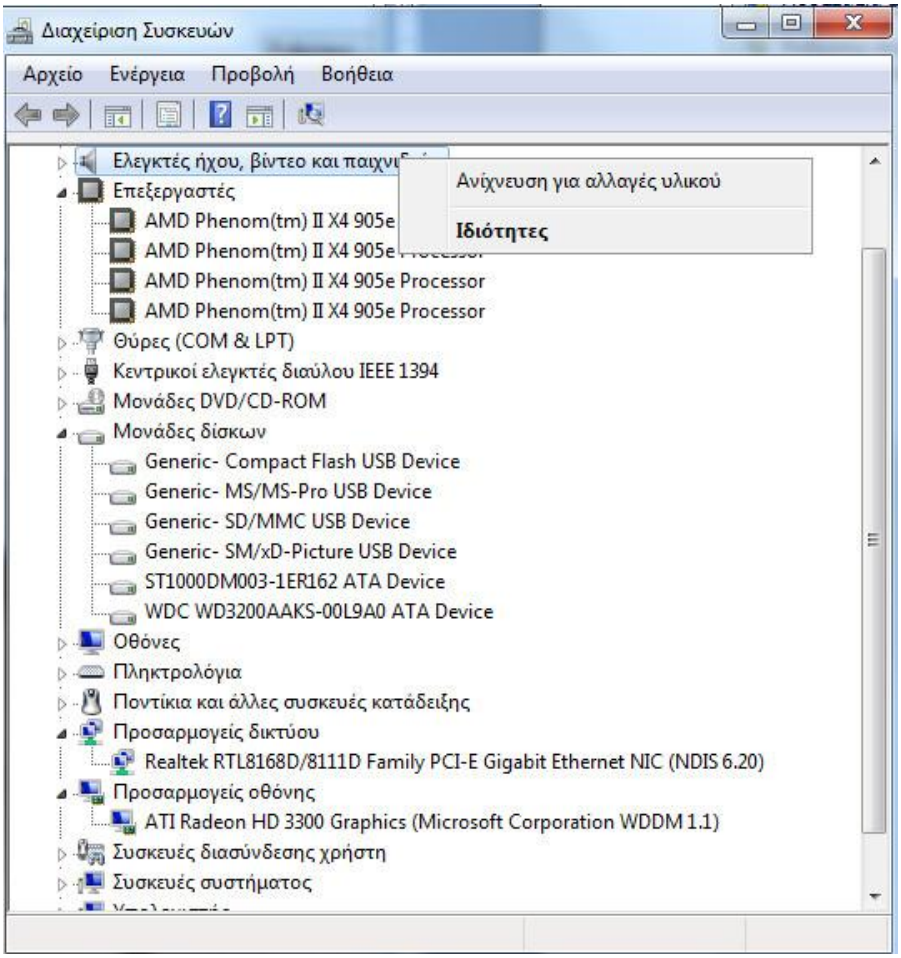
Για την περίπτωση εκείνη που η συσκευή που θέλουμε να συνδέσουμε σε έναν υπολογιστή είναι αρκετά παλιότερη ή νεότερη του λειτουργικού συστήματος θα πρέπει να προβούμε σε μία ή και στις δύο από τις παρακάτω ενέργειες:

1. *Ενημέρωση του λειτουργικού συστήματος.* Η διαδικασία αυτή επιβάλλεται γενικά να γίνεται ασχέτως αν εγκαθιστούμε συσκευές ή όχι, καθώς οι νέες ενημερώσεις του λειτουργικού συστήματος είναι δυνατόν, εκτός της υποστήριξης νέων συσκευών, να διορθώνουν ή να ανανεώνουν τμήματα του λειτουργικού συστήματος.
2. *Εγκατάσταση των οδηγών της συσκευής.* Η διαδικασία αυτή περιλαμβάνει την εγκατάσταση των προγραμμάτων οδήγησης (οδηγών) της συσκευής τα οποία παρέχονται από τον κατασκευαστή της συσκευής είτε άμεσα σε κάποιο αποθηκευτικό μέσο είτε μέσω διαδικτύου από την αντίστοιχη ιστοσελίδα υποστήριξης της συσκευής.

Στις περισσότερες περιπτώσεις η εγκατάσταση μιας νέας συσκευής είναι μια απλή υπόθεση. Είναι γνωστή άλλωστε η ορολογία Plug and Play (PnP, σύνδεσε και παίξε) που άρχισε να υπάρχει από την εποχή των Windows 98 και έπειτα. Υπάρχουν όμως και περιπτώσεις όπου η όλη αυτή διαδικασία μπορεί να γίνει αρκετά δύστροπη. Σε αυτές τις περιπτώσεις η ορολογία PnP μεταφράζεται (με δόση χιούμορ) σε Plug and Pray (σύνδεσε και προσευχήσου) αποδίδοντας έτσι την κατάσταση που μπορεί να δημιουργηθεί.

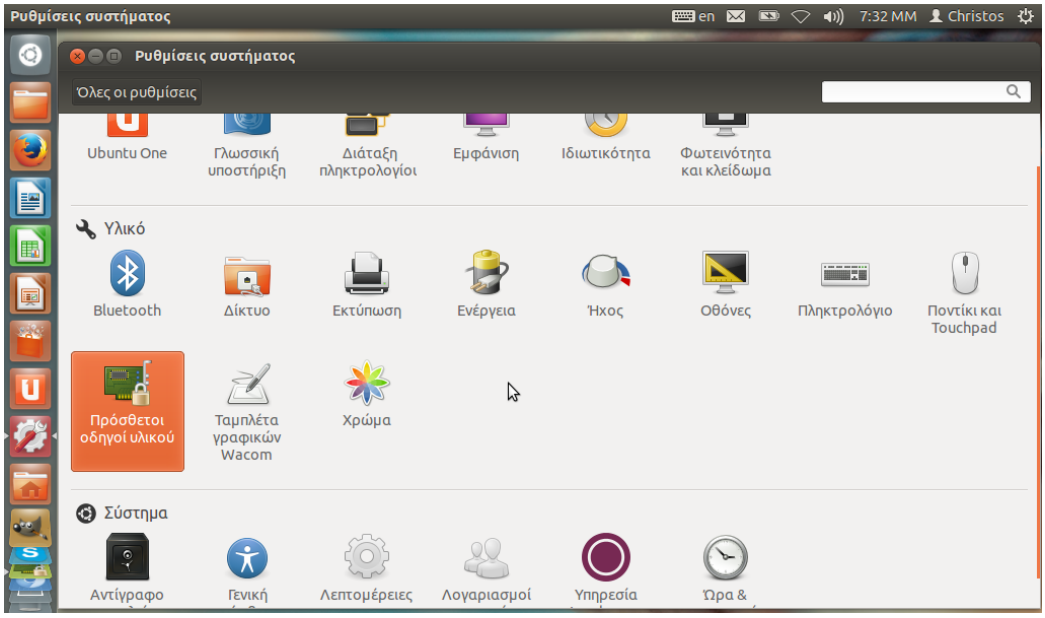
### 4.4 Διαχείριση των περιφερειακών συσκευών από το Λειτουργικό Σύστημα

Είδαμε ότι, όταν μια περιφερειακή συσκευή συνδεθεί σε μια υπολογιστική μονάδα, θα πρέπει να υπάρχει και το αντίστοιχο πρόγραμμα επικοινωνίας με αυτήν. Η κεντρική διαχείριση αυτών των προγραμμάτων γίνεται από το Λειτουργικό Σύστημα και υπάρχει πάντα ένας τρόπος καθορισμού της λειτουργίας τους ή της αναβάθμισής τους με νεότερα προγράμματα.

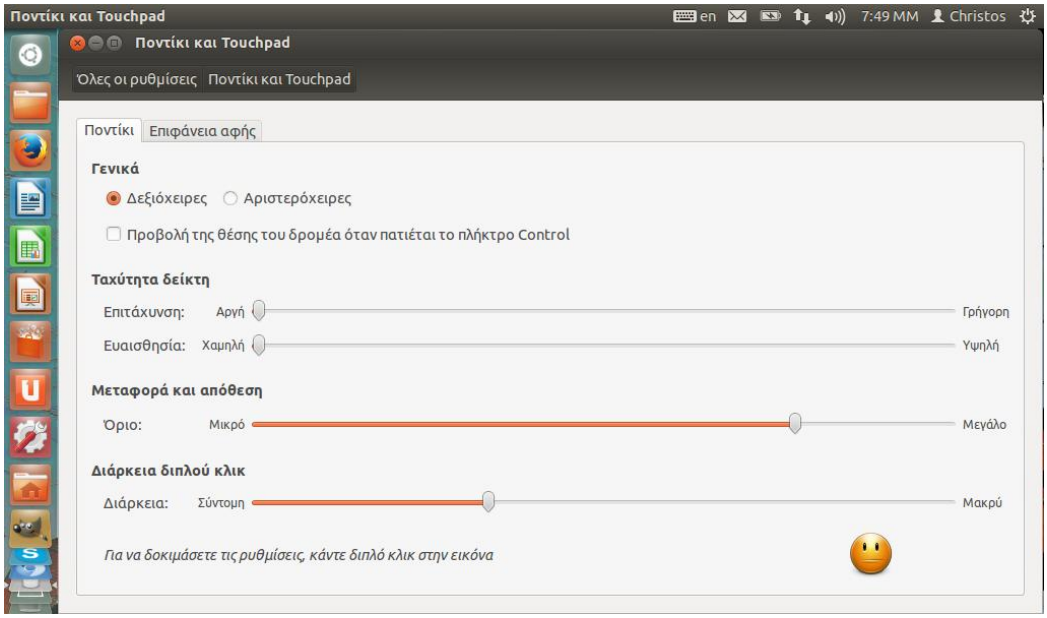



Εικόνα 4.3: Η διαχείριση συσκευών των Windows 7

Όπως αναφέρθηκε και στην προηγούμενη ενότητα, με την τεχνολογία PnP είναι δυνατή η αυτόματη ρύθμιση μιας περιφερειακής συσκευής, όσον αφορά στις διακοπές και στα κανάλια επικοινωνίας που θα χρειαστεί, έτσι ώστε να μην έρχεται σε συγκρούσεις με άλλες συσκευές. Όπως φαίνεται και στην εικ. 4.3, στη *Διαχείριση Συσκευών* εμφανίζονται όλες οι συσκευές που είναι συνδεδεμένες στον Η/Υ. Για το πρόγραμμα αυτό όλα είναι συσκευές, ακόμα και ο τετραπύρηνος επεξεργαστής όπως φαίνεται στην εικόνα ο οποίος αναγνωρίζεται ως τέσσερις διαφορετικές συσκευές. Με χειρισμούς από τη Διαχείριση Συσκευών μπορούμε να δούμε τις ιδιότητες τις συσκευής, τους πόρους που χρησιμοποιεί, τις τιμές των παραμέτρων της και άλλες ρυθμίσεις. Μπορούμε επίσης να κάνουμε κατάργηση της συσκευής ή αναβάθμιση των οδηγών της. Η αντίστοιχη δυνατότητα προσφέρεται σε γραφικό περιβάλλον στο Λειτουργικό Σύστημα Linux μέσω των ρυθμίσεων συστήματος όπως φαίνεται στις εικόνες 4.4 και 4.5 (για τη διανομή Ubuntu 12.04), ενώ υπάρχει πάντα και η δυνατότητα ρύθμισης και προβολής λεπτομερειών μέσω τις γραμμής εντολών (π.χ εντολή lspci, βλ. δραστηριότητα 9)




Εικόνα 4.4: Η διαχείριση συσκευών μέσω των ρυθμίσεων συστήματος στο Ubuntu 12.04




Εικόνα 4.5: Οι ρυθμίσεις παραμέτρων του ποντικιού στο Ubuntu 12.04

## Ερωτήσεις

1. Ποιο σύστημα μεταφέρει πληροφορίες και επιτρέπει τη σύνδεση περιφερειακών συσκευών σε έναν υπολογιστή;
2. Ποιος είναι ο τρόπος με τον οποίο μια περιφερειακή συσκευή ειδοποιεί το υπολογιστικό σύστημα για κάποιο συμβάν;
3. Ποιοι είναι οι τύποι των περιφερειακών συσκευών;
4. Υπάρχουν συσκευές που να είναι ταυτόχρονα εισόδου και εξόδου;
5. Τι απαιτείται για την επιτυχή σύνδεση και επικοινωνία της περιφερειακής συσκευής με το υπολογιστικό σύστημα;
6. Είναι αναγκαίο να εγκαθιστούμε πάντα χειροκίνητα τους οδηγούς μιας συσκευής;
7. Τι είναι καλό να γίνει πριν κάνουμε εγκατάσταση μιας συσκευής που είναι σχετικά πιο σύγχρονη από την υπολογιστική μονάδα μας;
8. Πως γίνεται η κεντρική διαχείριση των περιφερειακών συσκευών;

## Δραστηριότητες

**Windows**

1. Ελέγξτε τις συσκευές που είναι συνδεδεμένες στον υπολογιστή σας με βάση την διαχείριση συσκευών όπως φαίνεται στην εικ. 4.2
2. Καταργήστε μια συσκευή και μετά κάνετε αναζήτηση για νέες συσκευές.
3. Τοποθετήστε ένα οπτικό ποντίκι USB, τον εκτυπωτή του εργαστηρίου ή ένα flash disk στον υπολογιστή σας και παρατηρήστε τι θα συμβεί όσον αφορά τις αυτόματες διαδικασίες εγκατάστασης που θα εκκινήσουν.
4. Εξετάστε τις λεπτομέρειες κάποιας περιφερειακής συσκευής σας.
5. Ελέγξτε τους πόρους που χρησιμοποιεί η κάρτα γραφικών σας.
6. Εγκαταστήστε μια διαφορετική κάρτα γραφικών στον Η/Υ σας και προσπαθήστε να βρείτε τους κατάλληλους οδηγούς μέσω της σελίδας του κατασκευαστή της.

**Linux (ubuntu)**

7. Από τις *ρυθμίσεις συστήματος* (μέσω του εικονιδίου πάνω δεξιά) πηγαίνετε στο σύστημα και μετά στις λεπτομέρειες. Στο γραφικό περιβάλλον που εμφανίζεται εξερευνήστε τις συσκευές που φαίνονται εγκατεστημένες στο σύστημα σας.
8. Από τις ρυθμίσεις συστήματος και πάλι και μέσω του υλικού ελέγξτε τις δυνατότητες που σας δίνουν τα εκεί εικονίδια που αντιστοιχούν σε συσκευές.
9. Ανοίξτε ένα τερματικό και πληκτρολογήστε την εντολή lspci. Αναζητήστε πληροφορίες για τη χρήση της στο διαδίκτυο και ελέγξτε τις πληροφορίες για το δικό σας υπολογιστή.
10. Εκτελέστε τη δοκιμή συστήματος (system testing) και ελέγξτε τις πληροφορίες που είναι διαθέσιμες για τις συσκευές που είναι συνδεδεμένες στο σύστημα σας.

# 5. Ασφάλεια Πληροφοριακών Συστημάτων

Το κεφάλαιο αυτό είναι μια εισαγωγή στα βασικότερα σημεία της Ασφάλειας Πληροφοριακών Συστημάτων. Παρουσιάζει δηλαδή μια σφαιρική άποψη αυτού του τομέα της Πληροφορικής και δίνει βαρύτητα σε λύσεις που μπορούν να εφαρμοστούν στο σχολικό εργαστήριο.

**Διδακτικοί στόχοι**

Στο κεφάλαιο αυτό θα μάθετε για:

- το αντικείμενο της Ασφάλειας Πληροφοριακών Συστημάτων (Information Security System) και σημαντικά ιστορικά στοιχεία της.
- τα είδη των Χάκερς (hackers) και για το Ηλεκτρονικό έγκλημα.
- τις βασικές έννοιες της Ασφάλειας Πληροφοριακών Συστημάτων, όπως την τριάδα Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα και την ανάγκη ύπαρξης χρηστών με διαφορετικά δικαιώματα.
- τη Διαχείριση και Αξιολόγησης Κινδύνου καθώς και για το Σχέδιο Ασφαλείας με τις Πολιτικές Ασφαλείας και τα Αντίμετρα ασφαλείας.
- το Σχεδιασμό Επιχειρησιακής Συνέχειας και Επαναφοράς από Καταστροφή, με τη βοήθεια των Αντιγράφων Ασφαλείας.
- τα προβλήματα ασφαλείας του λογισμικού και τα διάφορα είδη κακόβουλου λογισμικού.
- την κρυπτογραφία και τη χρησιμότητά της.
- τα βασικότερα εργαλεία δικτυακής ασφάλειας.
- τους σπουδαιότερους τρόπους φυσικής ασφάλειας.

**Διδακτικές ενότητες**

5.1 Εισαγωγή

5.2 Βασικές Έννοιες

5.3 Ασφάλεια Λογισμικού

5.4 Ασφάλεια Δικτύου

5.5 Φυσική Ασφάλεια

## 5.1 Εισαγωγή

**5.1.1 Ιστορικά Στοιχεία για την Ασφάλεια Πληροφοριών.** Με την ανάπτυξη του ανθρώπινου πολιτισμού έγινε κατανοητό το πόσο σημαντική είναι η αποστολή μηνυμάτων με ασφάλεια, χωρίς να κινδυνεύει δηλαδή να μαθευτεί αλλά και να μην τροποποιηθεί το περιεχόμενο των μηνυμάτων.

Υπάρχουν γραπτές αναφορές από την αρχαία Ελλάδα και την Ρωμαϊκή εποχή για προστασία μηνυμάτων με την Κρυπτεία Σκυτάλη της αρχαίας Σπάρτης και τον Κώδικα του Καίσαρα στην Ρωμαϊκή εποχή.

Στη σύγχρονη εποχή, κατά τον Β' Παγκόσμιο Πόλεμο, έγινε γνωστή η συσκευή Αίνιγμα (Enigma), με την οποία αποστέλλονταν κρυπτογραφημένα μηνύματα από το ναζιστικό Γερμανικό στρατό. Η αποκρυπτογράφηση (σπάσιμο) των μηνυμάτων της με τη συμμετοχή του Άλαν Τούριγκ (Alan Turing) βοήθησε στην τελική έκβαση του πολέμου.

Αργότερα, τη δεκαετία του '80 και στην εποχή του ARPANET ακόμα, περιγράφηκε στο βιβλίο *The Cuckoo's Egg* (1989) του Κλιφ Στολ (Cliff Stoll) η ανακάλυψη και σύλληψη του Μάρκους Χες (Markus Hess) για ηλεκτρονική κατασκοπεία κατά του Αμερικανικού στρατού. Το 1988 ο Ρόμπερτ Μόρις (Robert Morris) δημιούργησε το πρώτο Σκουλήκι (worm) γνωστό ως Morris worm, το οποίο προξένησε προβλήματα σε χιλιάδες υπολογιστές και ήταν η αιτία δημιουργίας των Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας, γνωστών και ως CERT[1] (Computer Emergency Responce Team) στο πανεπιστήμιο Κάρνιγι Μέλον (Carnegie Mellon) του Πίτσμπουργκ (Pittsburgh) στις Ηνωμένες Πολιτείες Αμερικής. Εκείνη την εποχή φυλακίστηκε για πρώτη φορά και ένας από τους γνωστότερους μέχρι σήμερα χάκερς, ο Κέβιν Μίτνικ (Kevin Mitnick). Αυτός, κατά την περίοδο δράσης του είχε εισβάλει σε συστήματα των μεγαλυτέρων εταιριών της εποχής εκείνης, καθώς επίσης είχε υποκλέψει και στοιχεία εκατοντάδων πιστωτικών καρτών χρησιμοποιώντας την Κοινωνική Μηχανική (social engineering).

Σήμερα η εξάπλωση του διαδικτύου (internet) έχει φτάσει σε όλα τα μήκη και πλάτη της Γης. Μεταδίδονται μέσα από αυτό πληροφορίες με διάφορους τρόπους, από ιδιώτες και οργανισμούς, ενώ ταυτόχρονα υπάρχουν σ' αυτό ανταγωνιστές αλλά και διάφορες ομάδες ατόμων που καραδοκούν και συχνά το καταφέρνουν να υποκλέψουν δεδομένα και να τα εκμεταλλευτούν με διάφορους τρόπους.

### 5.1.2 Ορισμοί

**Πληροφοριακό Σύστημα (ΠΣ) - Information System (IS):** Είναι ένα σύνολο ανθρώπινου δυναμικού, υπολογιστών και διαδικασιών, τα οποία συνεργάζονται αρμονικά για να βοηθήσουν έναν οργανισμό να πετύχει τους στόχους του. (πχ το TAXIsnet του Υπουργείου Οικονομικών)

**Ασφάλεια Πληροφοριακών Συστημάτων – Information System Security:** Η Ασφάλεια Πληροφοριακών Συστημάτων είναι ένας τομέας της επιστήμης της Πληροφορικής, ο οποίος ασχολείται με την προστασία των δεδομένων ενός Πληροφοριακού Συστήματος από άτομα χωρίς εξουσιοδότηση.

[1] σήμερα λειτουργούν παγκοσμίως πάρα πολλές ομάδες. Στη χώρα μας υπάρχουν αρκετές μεταξύ των οποίων: του ΠΣΔ http://cert.sch.gr και του Ε.Δ.Ε.Τ. https://cert.grnet.gr)

Άτομο χωρίς εξουσιοδότηση είναι οποιοδήποτε δεν έχει άδεια πρόσβαση σε κάποιο τμήμα του πληροφοριακού συστήματος. Παραδείγματα τέτοιων τμημάτων μπορεί να είναι ένας φάκελος αρχείων, μια Βάση Δεδομένων κ.λπ.

**Ηλεκτρονικό Έγκλημα** (*ιστοσελίδα Ελληνικής Αστυνομίας*)**:** είναι οι αξιόποινες εγκληματικές πράξεις που τελούνται με την βοήθεια ηλεκτρονικών υπολογιστών και που τιμωρούνται από τη νομοθεσία. Ανάλογα με τον τρόπο που πραγματοποιούνται διαχωρίζονται σε εγκλήματα που έγιναν με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν έγιναν μέσω του Διαδικτύου. Αυτού του είδους τα εγκλήματα ονομάζονται Ηλεκτρονικά Εγκλήματα και τέτοια θεωρούνται τα παρακάτω:

- Τροποποίηση δεδομένων - Κλοπή δεδομένων
- Παρεμπόδιση κυβερνοκυκλοφορίας
- Εισβολή σε δίκτυο - Σαμποτάζ σε δίκτυο
- Μη εξουσιοδοτημένη πρόσβαση
- Διασπορά ιών - Υπόθαλψη αδικημάτων
- Πλαστογραφία - Απάτη

**Χάκερς (hackers):** αυτά τα άτομα ή ομάδες ατόμων, είναι συνήθως εξαιρετικά μεγάλη απειλή για δικτυωμένα συστήματα γιατί εισβάλουν μέσω του διαδικτύου. Έχουν βαθιές γνώσεις Λειτουργικών Συστημάτων (Operating Systems) και γλωσσών προγραμματισμού (Programming languages).

Ανάλογα με τις ηθικές τους αρχές χωρίζονται τουλάχιστον στις εξής 3 κατηγορίες, Black Hat / White Hat / Gray Hat:

- Οι **Black hats hackers** πολλές φορές λέγονται και κράκερς (Crackers) και συνήθως εισβάλουν σε συστήματα με σκοπό να κλέψουν, να καταστρέψουν δεδομένα, δημιουργούν κακόβουλο λογισμικό, σπάνε προγράμματα, υποκλέπτουν κωδικούς κ.λπ.
- Οι **White hats hackers** ψάχνουν για «κενά» (vulnerabilities) ασφαλείας σε Λειτουργικά Συστήματα, εφαρμογές και τους λόγους υπάρξεώς τους. Δεν έχουν σκοπό την καταστροφή δεδομένων και συνήθως ενημερώνουν τους υπεύθυνους για τα κενά ασφαλείας που βρίσκουν, ώστε να επιδιορθωθούν (ηθικό χάκινγκ).
- Μεταξύ Black και White Hats βρίσκονται οι **Gray hats hackers**. Είναι άτομα που χρησιμοποιούν τους υπολογιστές για να τιμωρήσουν υποτιθέμενους εγκληματίες του Κυβερνοχώρου (Cyberspace). Ονομάζονται και χακτιβιστές (hacktivists) όταν μεταφέρουν πολιτικά μηνύματα μέσω διαδικτύου.

**Κοινωνική Μηχανική (social engineering)**. Στον χώρο της Πληροφορικής έχει την έννοια της εξαπάτησης διαφόρων ατόμων, με σκοπό την απόσπαση εμπιστευτικών πληροφοριών. Οι πληροφορίες αυτές μπορεί να είναι προσωπικές, αλλά ενδέχεται να αφορούν και τον χώρο εργασίας. Ονόματα, ημερομηνίες γεννήσεως, κωδικοί, αριθμοί τηλεφώνων, ταχυδρομικές διευθύνσεις, ηλεκτρονικές διευθύνσεις (πολλές φορές οι χρήστες δίνουν τέτοια στοιχεία μέσω ιστοσελίδων Κοινωνικής Δικτύωσης) και τραπεζικά στοιχεία είναι κάποιες από τις πληροφορίες που ίσως είναι στόχος των ενδιαφερομένων. Τέτοια στοιχεία μπορούν να χρησιμοποιηθούν, για παράδειγμα σε διαδικτυακές αγορές ή να πουληθούν σε τρίτους ή για εκφοβισμό και για εκβιασμό των ιδιοκτητών τους.

Η γνωστότερη τεχνική που χρησιμοποιούν για την απόσπαση πληροφοριών είναι το *ηλεκτρονικό ψάρεμα (phishing),* όπου συνήθως χρησιμοποιούνται πλαστά ηλεκτρονικά μηνύματα (πχ. από τράπεζες) και σύνδεσμοι προς πλαστές ιστοσελίδες και ζητούν την καταχώρηση των πληροφοριών που τους ενδιαφέρουν.

## 5.2 Βασικές Έννοιες

**5.2.1 Απειλές κατά των Δεδομένων** Απειλή λέγεται καθετί που μπορεί να συμβεί από εσωτερικό ή εξωτερικό παράγοντα, φυσική καταστροφή, ανθρώπινο λάθος, λογισμικό (πχ. κακόβουλο λογισμικό ή κενό ασφαλείας του), εισχώρηση στο δίκτυο, και να προκαλέσει πρόβλημα σ' έναν οργανισμό. Μερικά προβλήματα που μπορούν να προκληθούν είναι τα εξής: διαρροή πληροφοριών, τροποποίηση δεδομένων ή η αναστολή λειτουργίας κάποιου υπολογιστικού συστήματος, όπως ένας διακομιστής ιστοσελίδων. Εάν συμβεί κάτι από αυτά τότε ανάλογα με το είδος των πληροφοριών (π.χ. ιατρικές εξετάσεις, σχέδια ενός μηχανήματος κ.λπ.), μπορεί να προκληθούν προβλήματα οικονομικά και κοινωνικά σε ιδιώτες και επιχειρήσεις.

**5.2.2 Βασικές Αρχές Ασφαλείας Πληροφοριακών Συστημάτων.** Η Ασφάλεια Πληροφοριακών Συστημάτων στηρίζεται σε τρεις βασικές αρχές απαραίτητες για την σωστή λειτουργία των Πληροφοριακών Συστημάτων. Αυτές είναι η τριάδα Εμπιστευτικότητα-Ακεραιότητα-Διαθεσιμότητα ΕΑΔ - (Confidentiality-Integrity-Availability – CIA triad). Συγκεκριμένα:

1. **Εμπιστευτικότητα (confidentiality)**
   Στόχος της είναι η εξασφάλιση πως τα δεδομένα δε θα γίνουν διαθέσιμα, δε θα μπορούν να τα διαβάσουν δηλαδή, μη εξουσιοδοτημένα άτομα.

   Τα δεδομένα θα πρέπει να κατηγοριοποιούνται ανάλογα με την σημαντικότητά τους. Ανάλογα δηλαδή με το τι επιπτώσεις θα έχει η εμφάνισή τους σε λάθος άτομα. Έτσι, θα μπορούν να μπουν διαφορετικοί περιορισμοί σε κάθε κατηγορία που θα δημιουργηθεί.

   Όσο σημαντικότερα είναι αυτά που πρέπει να προστατευτούν τόσο ισχυρότερα μέτρα θα πρέπει να λαμβάνονται (πχ απομόνωση από το δίκτυο συστημάτων με κρίσιμα δεδομένα, τοποθέτηση επιπλέον μέτρων προστασίας, απενεργοποίηση USB θυρών, κρυπτογράφηση και σε ακραία περίπτωση θα μπορούν να υπάρχουν μόνο τυπωμένα όσα θέλουμε να προστατευτούν πχ: σχέδια, οδηγίες κ.λπ.)

2. **Ακεραιότητα (integrity)**
   Η αρχή της Ακεραιότητας εξασφαλίζει πως τα δεδομένα δε θα υποστούν καμία αλλοίωση από μη εξουσιοδοτημένα άτομα ή με μη ανιχνεύσιμο τρόπο. Σε περιπτώσεις τροποποίησης θα πρέπει να παράγονται σχετικά μηνύματα ειδοποίησης (π.χ. με χρήση ελέγχου αθροίσματος MD5, Αντιγράφων ασφαλείας κ.λπ.)

3. **Διαθεσιμότητα (Availability)**
   Αυτή εξασφαλίζει πως το σύστημα θα μπορεί να παρέχει τις πληροφορίες του, όταν του ζητηθούν και μέσα σε αποδεκτά χρονικά όρια.

   Υπολογιστές, δίκτυα και συσκευές δικτύου θα πρέπει να επιδιορθώνονται όσο γίνεται γρηγορότερα. (π.χ. με Σχέδιο Αποκατάστασης από Καταστροφή - Disaster Recovery Plan και Σχέδιο Επιχειρησιακής Συνέχειας - Business Continuity)

**5.2.3 Έλεγχος Πρόσβασης (Access Control).** Για να μπορέσει ένας οργανισμός να προστατεύσει τις πληροφορίες του από τυχαίες ή εσκεμμένες αλλοιώσεις εξουσιοδοτημένων και από εσκεμμένες αλλοιώσεις από μη εξουσιοδοτημένα άτομα θα πρέπει να εφαρμόσει ελέγχους πρόσβασης στα συστήματα και τους δικτυακούς του πόρους.

Ο έλεγχος πρόσβασης εφαρμόζεται σε τρεις περιπτώσεις:

1. **Δικτυακή πρόσβαση**: οι χρήστες έχουν την δυνατότητα πρόσβασης σ' όλους τους πόρους του δικτύου. Για το λόγο αυτό θα πρέπει στους πόρους του δικτύου να μπουν περιορισμοί (πχ ποιος-τι), να προστατευτούν και να παρακολουθούνται. Οι χρήστες του Τμήματος Προσωπικού για παράδειγμα, δε θα πρέπει να έχουν πρόσβαση στο δίκτυο του Οικονομικού Τμήματος ενός οργανισμού.
2. **Πρόσβαση σε συστήματα**: οι χρήστες χρησιμοποιούν διάφορα συστήματα του δικτύου όπως διακομιστές (servers), εκτυπωτές (printers) αλλά και κάθε άλλο είδος διαμοιραζόμενης συσκευής (shared device) στο δίκτυο. Η πρόσβαση σ' αυτές τις συσκευές θα πρέπει να περιορίζεται, να προστατεύεται και να παρακολουθείται.
3. **Πρόσβαση στα δεδομένα**: οι χρήστες έχουν πρόσβαση στα δεδομένα του δικτύου. Διαβάζουν και τροποποιούν αρχεία (files) και Βάσεις Δεδομένων (Databases). Τα δεδομένα θα πρέπει να υπόκεινται σε περιορισμούς, προστασία και παρακολούθηση.

Ο Έλεγχος Πρόσβασης είναι σημαντικότατος για επιχειρήσεις, κυβερνητικούς οργανισμούς και χρησιμοποιείται για να αποτρέπονται απάτες και λάθη. Για παράδειγμα, θα δημιουργηθεί πρόβλημα, εάν τροποποιηθούν στοιχεία μιας τράπεζας ή τα στοιχεία ενός ληξιαρχείου.

Η Ακεραιότητα Δεδομένων θα πρέπει να προστατεύεται, δίνοντας δικαιώματα πρόσβασης σε πόρους με βάση τις αρχές: Χρειάζεται-Να-Ξέρω (need-to-know) και Χρειάζεται-Να-Κάνω (need-to-do).

Τα δικαιώματα χρηστών θα πρέπει να χορηγούνται ανάλογα με τον ρόλο τους, τις ευθύνες τους και τις εργασίες που εκτελούν μέσα στον οργανισμό.

Οι πόροι θα πρέπει να κατηγοριοποιούνται σε επίπεδα. Για παράδειγμα ένα έγγραφο μπορεί να χαρακτηριστεί Απόρρητο, Εμπιστευτικό, Δημόσιο.

Θα πρέπει να υπάρχουν Αρχεία Καταγραφής συμβάντων (Log files) ώστε σε περίπτωση πχ απάτης ή απώλειας να μπορεί να αναζητηθεί η πηγή (πχ Η/Υ ή χρήστης) που την προκάλεσε και να τιμωρηθεί ο ένοχος.

Θα πρέπει λοιπόν να χορηγούνται δικαιώματα με σύνεση για να διασφαλιστεί η προστασία των δεδομένων.

**5.2.3.1 Πιστοποίηση Ταυτότητας (Authentication) και Εξουσιοδότηση (Authorization). Πιστοποίηση Ταυτότητας** είναι η διαδικασία ταυτοποίησης και επιβεβαίωσης πως κάποιος έχει εξουσιοδότηση πρόσβασης στους δικτυακούς πόρους του οργανισμού, κάτι ανάλογο με το να δείξουμε την αστυνομική μας ταυτότητα για να μπούμε σε κάποιο φυλασσόμενο κτίριο. Στην πληροφορική αυτό γίνεται συνήθως με το Όνομα Χρήστη (username) και με τον κωδικό του (password). Δεν είναι ο ασφαλέστερος τρόπος και υπάρχουν πολλοί άλλοι, για παράδειγμα με βιομετρικά στοιχεία (δακτυλικό αποτύπωμα, ίριδα ματιού κ.λπ.).

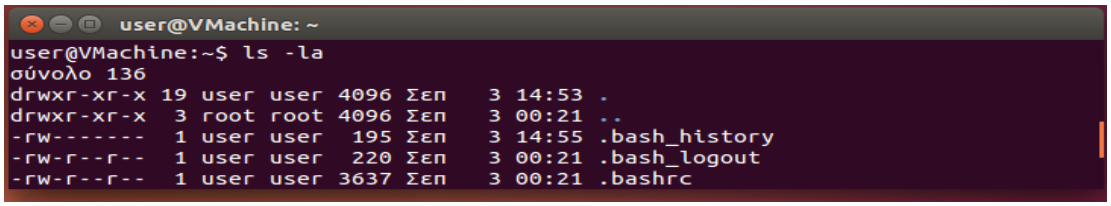
**5.2.3.2 Εφαρμογή Έλεγχου Πρόσβασης.** Δύο διαδομένες μορφές υλοποίησης Ελέγχου Πρόσβασης είναι οι Λίστες Ελέγχου Πρόσβασης και αυτή του Active Directory (AD) ή του LDAP

**Λίστες Ελέγχου Πρόσβασης (Access Control Lists ή ACL)**

Με τις Λίστες Ελέγχου Πρόσβασης (ACL) σε κάθε πόρο του δικτύου ή του συστήματος μπορούν να εφαρμοστούν δύο βασικοί κανόνες: επιτρέπεται (allow) και δεν επιτρέπεται (deny). Παράδειγμα, ο χρήστης user1 επιτρέπεται να έχει πρόσβαση στον διακομιστή-Α ενώ ο χρήστης user2 δεν επιτρέπεται.

Οι ACL μπορούν να εφαρμοστούν σε συστήματα αρχείων (file systems) και σε δίκτυα (networks):

1. ACL συστήματος αρχείων. Τα αρχεία έχουν τριών ειδών δικαιώματα: Ανάγνωσης (Read), Εγγραφής (Write) και Εκτέλεσης (eXecute) που επιτρέπουν τις ανάλογες ενέργειες πάνω στα αρχεία. Τα δικαιώματα μπορούν να δοθούν σε χρήστες και σε ομάδες (σε ΛΣ Linux με την εντολή *chmod* – εικ. *5.1*)
2. ACL δικτύου: με τις ACL μπορούν να δοθούν δικαιώματα πρόσβασης στους πόρους του δικτύου. Λειτουργούν σαν φίλτρα και μπορούν να ελέγχουν την κίνηση ΑΠΟ και ΠΡΟΣ το δίκτυο του οργανισμού.




Εικόνα 5.1: Εμφάνιση δικαιωμάτων, ιδιοκτήτη, ομάδας σε Linux

Οι ACL χρησιμοποιούνται από δικτυακές συσκευές όπως Δρομολογητές (Routers), Μεταγωγείς (Switches) αλλά και προγράμματα επιβολής δικτυακών περιορισμών όπως Τείχη Προστασίας (firewalls) και Διακομιστές Διαμεσολάβησης (Proxy servers). Η γενική μορφή σύνταξης μιας ACL δικτύου περιλαμβάνει: τον κανόνα Permit/Deny, IP πηγής, IP προορισμού, τύπος πρωτοκόλλου (TCP,UDP,IP κ.λπ.).

Για παράδειγμα, όταν φτάσει ένα πακέτο (packet) στον Δρομολογητή αυτός ελέγχει τις ACL για να δει ποια θα εφαρμοστεί στην περίπτωσή του και ανάλογα μετά απορρίπτεται (dropped) ή επιτρέπεται (permitted) η διέλευσή του.

πχ. *ACL Cisco router : access-list 101 10.147.63.* 10.148.64.* permit tcp*

Οι ACL υλοποιούνται στο Επίπεδο Δικτύου του TCP/IP και του OSI.

**Active Directory (AD) και LDAP**

Το **LDAP** (Lightweight Directory Access Protocol) είναι ανοιχτού κώδικα (open source) και ορίζει τον τρόπο που οι πληροφορίες του οργανισμού μπορούν να προσπελαθούν από τον καθένα. Χρησιμοποιείται για την αποθήκευση πληροφοριών Πιστοποίησης Ταυτότητας, Εξουσιοδότησης των χρηστών αλλά και Ρόλων.

Λειτουργεί με το μοντέλο πελάτη/εξυπηρετητή (Client/Server). Οι πελάτες για να αποκτήσουν πρόσβαση στους πόρους του δικτύου και σε εφαρμογές, θα πρέπει πρώτα να Πιστοποιήσουν την Ταυτότητά τους στον LDAP Server, για να τους δώσει εξουσιοδότηση χρήσης τους.

Το **Active Directory** (AD) είναι αναπτυγμένο από την Microsoft και παρέχει υπηρεσίες Πιστοποίησης Ταυτότητας και Εξουσιοδότησης. Έχει κεντρική διαχείριση και αποθηκεύει πληροφορίες Χρηστών, Ομάδων, Συστημάτων και πόρων ως αντικείμενα (Objects). Τα

αντικείμενα αυτά οργανώνονται σε Οργανικές Μονάδες (Organizational Units – OU) και μπορούν να εφαρμοστούν πάνω τους πολιτικές δικαιωμάτων.

**5.2.4 Διαχείριση Ασφαλείας Πληροφοριακού Συστήματος.** Η Διαχείριση Ασφαλείας Πληροφοριακού Συστήματος έχει ως σκοπό την προστασία των Πληροφοριακών Συστημάτων περιορίζοντας την επικινδυνότητα παραβίασης κάποιας από τις τρεις Βασικές Αρχές ΕΑΔ σε αποδεκτό όριο.

Οι διαδικασίες που περιλαμβάνει συνοπτικά είναι:

1. Η Διαχείριση Κινδύνου, για να προσδιοριστή το αποδεκτό επίπεδο ασφαλείας
2. Η ανάπτυξη και εφαρμογή Σχεδίου Ασφαλείας με την οποία θα μπορεί να επιτευχθεί το επιθυμητό επίπεδο ασφάλειας
3. Η Επαναφορά από Καταστροφή και η Επιχειρησιακή Συνέχεια

**5.2.4.1 Διαχείριση Κίνδυνου ή Επικινδυνότητας (Risk Management).** Η Διαχείριση Κινδύνου ή Επικινδυνότητας είναι μια διαδικασία αναγνώρισης (ανεύρεσης):

a) **Ευπαθειών (vulnerabilities)** και **Απειλών (threats)** στις οποίες μπορούν εκτεθούν οι πληροφορίες που χρησιμοποιεί και παρέχει ένα Πληροφοριακό Σύστημα, καθώς και
b) των **Αντιμέτρων (Countermeasures)** ή **Μέτρων Ασφαλείας (Security Measures)** ή **Μέτρων Προστασίας (Controls)** που θα παρθούν για να μειωθεί ο κίνδυνος αλλοίωσης των πληροφοριών αυτών.

Η ανάλυση και εκτίμηση κινδύνου κάθε τμήματος του Πληροφοριακού Συστήματος γίνεται βάση τη μέθοδο που θα επιλέξει ο οργανισμός.

Η **Αξιολόγηση Κινδύνου (Risk Assessment)** θα προσδιορίσει τις πιθανές ζημιές που μπορεί να προκαλέσει κάθε Απειλή, σε σχέση με το κόστος των προληπτικών μέτρων για την αντιμετώπισή του. Με τον τρόπο αυτό μπορεί να προσδιοριστεί το συνολικό ποσό που θα χρειαστεί για την προστασία του Πληροφοριακού Συστήματος.

Η Διαχείριση Κινδύνου έναντι Απειλών, συνυπολογίζει την πιθανότητα πραγματοποίησης μιας Απειλής, καθώς και το τι επιπτώσεις θα έχει αυτή στην ομαλή λειτουργία της επιχείρησης, αλλά και το πόσο θα κοστίσει στην επιχείρηση η ζημιά από την πραγματοποίηση της Απειλής.

Σε περίπτωση μιας απειλής με μικρό αντίκτυπο και μικρή πιθανότητα πραγματοποίησης, ο οργανισμός μπορεί να την αφήσει να υπάρχει και να μην πάρει μέτρα (accept the risk). Με παρόμοιο τρόπο κρίνονται όλες οι απειλές, οπότε στο τέλος θα επιλεχθούν τα Αντιμέτρα που θα εφαρμοστούν για την ασφάλεια του ΠΣ.

Μέθοδοι Διαχείρισης Κινδύνου είναι η OCTAVE, CMU, ISO/IEC 31000:2009 και πολλές άλλες ακόμα.

Οι Απειλές και οι Ευπάθειες μεταβάλλονται με την πάροδο του χρόνου, επομένως η διαδικασία αναγνώρισής τους είναι μια διαδικασία που δε γίνεται μόνο μια φορά, αλλά επαναλαμβάνεται συχνά.

Για την καλύτερη κατανόηση θα πρέπει να δώσουμε εδώ τους εξής ορισμούς:

- **Κίνδυνος**: είναι η πιθανότητα μια απειλή να γίνει πραγματικότητα.

- **Αντίμετρα (Countermeasures)** ή **Μέτρα Ασφαλείας (Security Measures)** ή **Μέτρα Προστασίας (Controls)**: είναι το μέτρα που λαμβάνονται για την αντιμετώπιση μιας απειλής σε ένα Πληροφοριακό Σύστημα.
- **Απειλή (Threat):** είναι καθετί που μπορεί να συμβεί από ανθρώπινο παράγοντα (πχ. λάθος χειρισμός), φυσικό συμβάν (πχ. πλημμύρα) ή λογισμικό (πχ. κακόβουλο λογισμικό) και να παρακάμψει κάποια από τις τρεις Βασικές Αρχές: Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα του Πληροφοριακού Συστήματος.
- **Ευπάθεια (Vulnerability)**: είναι οι αδυναμίες που μπορεί να υπάρξουν σ' ένα Πληροφοριακό Σύστημα και επιτρέπουν να γίνει κάποια Απειλή πραγματικότητα. Τέτοιες αδυναμίες μπορεί να υπάρξουν για παράδειγμα: στις ρυθμίσεις παραμέτρων του δικτύου, σε εγκατεστημένα προγράμματα, στον τρόπο που λειτουργεί ο οργανισμός κ.λπ.

**Παραδείγματα**:

1. **Απειλή**: να τεθεί ένας Εξυπηρετητής (Server) μη διαθέσιμος. **Ευπάθεια**: μικρό εύρος γραμμής (bandwidth) και λήψη πάρα πολλών αιτήσεων για την εμφάνιση της ιστοσελίδας του οργανισμού.
2. **Απειλή**: να επιτραπεί σε όλους η λήψη ενός ηλεκτρονικού βιβλίου που πουλάει ο οργανισμός μέσω της ιστοσελίδας του. **Ευπάθεια**: λανθασμένες ρυθμίσεις στον Εξυπηρετητή Ιστοσελίδων επιτρέπουν τη λήψη του από όλους (Public Access)

**5.2.4.2 Σχέδιο Ασφάλειας (Security Plan).** Το Σχέδιο Ασφαλείας είναι ένα έγγραφο που αποτελείται από το άθροισμα των *(Α) Πολιτικών Ασφαλείας* και *(Β) των Μέτρων Ασφαλείας (Controls) ή Αντιμέτρων (Countermeasures)* που εφαρμόζονται σε ένα Πληροφοριακό Σύστημα.

**Α) Πολιτική Ασφαλείας (Security Policy).** Η Πολιτική Ασφαλείας ενός Πληροφοριακού Συστήματος είναι ένα έγγραφο στο οποίο περιγράφονται οι στόχοι της ασφάλειας, η προστασία του Πληροφοριακού Συστήματος, και οι διαδικασίες που πρέπει να ακολουθούνται από όλους, ώστε να επιτευχθούν αυτοί οι στόχοι.

Για να δημιουργηθεί η Πολιτική Ασφαλείας θα πρέπει να εντοπιστούν και να χαρακτηριστούν με έναν βαθμό εμπιστευτικότητας οι πληροφορίες που θα πρέπει να προστατευτούν. Στη συνέχεια θα πραγματοποιηθεί διαδικασία Διαχείρισης Κινδύνου (ή Επικινδυνότητας) και τα αποτελέσματά της θα χρησιμοποιηθούν, ώστε να επιλεχθούν τα κατάλληλα Αντίμετρα Ασφαλείας για την προστασία των κρίσιμων πληροφοριών του συστήματος.

Η Πολιτική Ασφαλείας ενός οργανισμού θα πρέπει να ικανοποιεί:

- Τη διοίκησή του.
- Τα μέλη του.
- Τους πελάτες του, γιατί δεδομένα τους θα αποθηκεύονται στο Πληροφοριακό Σύστημα. (Παράδειγμα: εάν το ΠΣ κρατά ιατρικές εξετάσεις ασθενών, τότε θα χρειάζονται διαβεβαίωση πως αυτά θα είναι ασφαλή και δεν θα διαρρεύσουν σε τρίτους).
- Τους **νομικούς περιορισμούς** και υποχρεώσεις που ισχύουν για την λειτουργία του οργανισμού.

**Β) Αντίμετρα (Countermeasures) ή Μέτρα Ασφαλείας (Security Measures) ή Έλεγχοι (Controls)**

Για να ικανοποιηθούν οι απαιτήσεις ασφαλείας του ΠΣ και να μειωθεί η επικινδυνότητα στο επιθυμητό επίπεδο σχεδιάζονται μέτρα που καλύπτουν τις παρακάτω κατηγορίες:

1. **Διοικητικά μέτρα (administrative)** (οργάνωση και διαχείριση της Ασφάλειας του ΠΣ) περιγράφονται: οι ρόλοι και οι αρμοδιότητες του προσωπικού, ο τρόπος διαχείρισης πληροφοριών, ο κώδικας δεοντολογίας (εσωτερικών κανόνων), η εκπαίδευση χρηστών για τις λειτουργίες του Π.Σ, η διαδικασία πρόσληψης και αποχώρησης υπαλλήλου (πχ δέσμευση εμπιστευτικότητας), και η διαβάθμιση πληροφοριών
2. **Τεχνικά μέτρα**: έλεγχος πρόσβασης (διαχείριση χρηστών, συνθηματικών), ασφάλεια επικοινωνιών, λειτουργία των αρχείων καταγραφής (log files) και διαδικασία λήψης αντιγράφων ασφαλείας (Backup), αποσπώμενα μέσα αποθήκευσης, μέτρα για την διαχείριση και υποστήριξη προμήθειας Λογισμικού και Υλικού, μέτρα ανάπτυξης και συντήρησης εφαρμογών (ασφαλής δοκιμές τους), απογραφή λογισμικού και υλικού, αδιάλειπτη παροχή ρεύματος (UPS) και τρόπο διαχείρισης περιστατικών ασφαλείας (security incident).
3. **Μέτρα φυσικής ασφάλειας**: από φυσικές καταστροφές, ασφάλεια πρόσβασης στις κτιριακές εγκαταστάσεις, υπολογιστικού και δικτυακού εξοπλισμού (πχ κλειδαριές με συρματόσχοινο)

Για να είναι αποτελεσματικά τα Μέτρα Ασφαλείας ή Αντίμετρα, θα πρέπει να εφαρμόζονται σωστά. Παράγοντες που επηρεάζουν την εφαρμογή τους είναι:

a) Η κατανόηση από μέρους των χρηστών της σημαντικότητας χρήσης τους.
b) Ο τακτικός έλεγχος της αποτελεσματικότητας και της εφαρμογής τους.
c) Η εύκολη χρήση τους από τους χρήστες.

**5.2.4.3 Σχεδιασμός Επαναφοράς από Καταστροφή (Disaster Recovery) και Επιχειρησιακής Συνεχείας (Business Continuity)**. Οι καταστροφές που μπορούν να συμβούν σε έναν οργανισμό από φυσικά φαινόμενα ή από τον ανθρώπινο παράγοντα είναι πιθανό να είναι τόσο σημαντικές, ώστε να υποχρεωθεί αυτός να διακόψει τη λειτουργία του για απροσδιόριστο χρονικό διάστημα.

Καταστροφές από ανθρώπινο παράγοντα μπορεί είναι:

- κακόβουλες ενέργειες,
- λάθη,
- εμπρησμοί,
- τρομοκρατικές ενέργειες,

Καταστροφές από φυσικά φαινόμενα:

- πλημμύρες
- σεισμοί
- κεραυνοί

Είναι προφανές πως, εάν ένας οργανισμός δεν έχει κάνει τις απαραίτητες ενέργειες κατά τη διάρκεια λειτουργίας του, τότε θα αντιμετωπίσει τεράστια προβλήματα σε περίπτωση που υποστεί κάποια σοβαρή καταστροφή.

**Σχεδιασμός Επιχειρησιακής Συνέχειας (Business Continuity)** είναι μεθοδολογία που θα χρησιμοποιηθεί για να κρατήσει την επιχείρηση σε λειτουργία.

**Η Ανάκαμψη ή Επαναφορά από Καταστροφή (Disaster Recovery)** είναι υποσύνολο της Επιχειρησιακής Συνέχειας και έχει ως σκοπό την όσο γίνεται γρηγορότερη αντιμετώπιση των συνεπειών μιας καταστροφής για να μπορέσει να λειτουργήσει η επιχείρηση.

Ακολουθώντας τα βήματα της μεθοδολογίας που επιλέχθηκε, θα καταρτιστούν τα ανάλογα έγγραφα. Το Σχέδιο Επιχειρησιακής Συνέχειας και με παρόμοια σχεδόν βήματα το Σχέδιο Ανάκαμψης από Καταστροφή. Σε αυτά θα περιγράφονται ποιες ενέργειες και το πότε θα πραγματοποιηθούν αυτές μετά από μια καταστροφή, τι αρμοδιότητες θα έχουν τα μέλη της ομάδας και το πώς θα επικοινωνούν μεταξύ τους.

Η ενημέρωση του σχεδίου θα πρέπει να ελέγχεται κατά διαστήματα για να εξακριβώνεται εάν συμπεριλαμβάνονται τυχόν αλλαγές στον οργανισμό και αν αυτό είναι ακόμα εφαρμόσιμο.

**Αντίγραφα Ασφαλείας (backup):** ένα σύστημα μπορεί να καταρρεύσει για διάφορους λόγους, όπως είναι για παράδειγμα πρόβλημα σε σκληρό δίσκο του και ίσως χαθούν και δεδομένα του μετά από αυτό. Η λήψη αντιγράφων ασφαλείας με σωστό τρόπο είναι απαραίτητη, γιατί αυτό θα βοηθήσει στο να επιτευχθεί γρηγορότερα διαθεσιμότητα του συστήματος αλλά και της ακεραιότητας των δεδομένων του. Η διαδικασία κατά την οποία χρησιμοποιούνται τα αντίγραφα ασφαλείας για να διορθωθούν προβλήματα λέγεται **επαναφορά** (**restore**).

Ανάλογα με την κρισιμότητα των δεδομένων του ο οργανισμός αναπτύσσει την στρατηγική λήψης αντιγράφων ασφαλείας. Για παράδειγμα μια τράπεζα ή μια εταιρία κρατήσεων εισιτηρίων θα πρέπει να μπορεί να είναι λειτουργία όσο γίνεται γρηγορότερα σε περίπτωση κάποιας καταστροφής. Η μη διαθεσιμότητα των συστημάτων τους για μεγάλο διάστημα ή η απώλεια δεδομένων (ακεραιότητας) θα επηρεάσει αρνητικά την φήμη τους. Για να επιτευχθεί υψηλή διαθεσιμότητα (high availability) θα πρέπει να χρησιμοποιηθούν συστήματα όπως: συστοιχίες δίσκων σε RAID, καθρεπτισμός διακομιστών (server mirroring), remote journaling, Storage Area Network (SAN). Οι επιλογές αυτές μπορούν να συμβάλουν στο να υπάρξει ταχύτατη επαναφορά των συστημάτων και της επιχειρησιακής συνέχειας. Μερικές από τις παραπάνω λύσεις είναι πολύ ακριβές καθώς πέρα από το κόστος του εξοπλισμού, χρειάζονται επιπλέον προσωπικό και χώρους.

Κάθε οργανισμός θα πρέπει να κρατά τουλάχιστον ένα είδος αντιγράφων ασφαλείας ακόμα και σε μέσα αποθήκευσης μικρής ταχύτητας (μαγνητικές ταινίες). Ένα τυπικό είδος αντιγράφων ασφαλείας σε σετ ταινίες[2] μπορεί να περιλαμβάνει:

1. **Πλήρες** (ολόκληρου του συστήματος) εβδομαδιαίο αντίγραφο ασφαλείας - (full backup) σε μαγνητικές ταινίες (tapes). Συνήθως επανεγγράφονται την αντίστοιχη βδομάδα του επόμενου μήνα.
2. Μηνιαίο ή ετήσιο (αποθήκευσή τους για αρκετά χρόνια).
3. και πρόσθετα καθημερινό **διαφορικό** (**differential**) **ή αυξητικό** (**incremental**) αντίγραφο ασφαλείας (**<u>όχι και τα δυο</u>**). Η διαφορά τους είναι η εξής:

[2] Για περισσότερες λεπτομέρειες επισκεφτείτε την 20η και 21η ιστοσελίδα της *Δικτυογραφίας.*

Έστω πως το Σαββατοκύριακο έγινε το πλήρες αντίγραφο ασφαλείας. Την Δευτέρα τροποποιήθηκε το αρχείο Α, την Τρίτη το αρχείο Β και την Τετάρτη το αρχείο Γ. Το αυξητικό αντίγραφο ασφαλείας της Δευτέρας θα πάρει το Α, της Τρίτης θα πάρει μόνο το Β και της Τετάρτης θα πάρει μόνο το Γ. Το διαφορικό αντίγραφο ασφαλείας της Δευτέρας θα πάρει το Α, της Τρίτης θα πάρει το Α και το Β, της Τετάρτης θα πάρει το Α το Β και το Γ.

Τα Αντίγραφα Ασφαλείας θα πρέπει:

1. να κρυπτογραφούνται αν χρειάζεται
2. να μην χαθεί ποτέ κανένα
3. να προστατεύονται από φωτιά, νερό κ.λπ.
4. να βρίσκονται σε διαφορετική τοποθεσία από αυτήν του οργανισμού. Για να επιλέξει την καταλληλότερη τοποθεσία πρέπει να εξετάζει τα παρακάτω:
   - η περιοχή αποθήκευσης να βρίσκεται σε ασφαλή απόσταση, ώστε να μην επηρεαστούν σε περίπτωση καταστροφής
   - να μπορούν να ανακτηθούν γρήγορα από την απομακρυσμένη περιοχή
   - την ασφάλεια του χώρου
   - το κόστος

Ανάλογα με το είδος του οργανισμού είναι πιθανό να χρειαστούν εναλλακτικές εγκαταστάσεις προκειμένου να μπορέσει να ανακάμψει πλήρως και γρήγορα από μια καταστροφή. Αυτές οι εγκαταστάσεις μπορεί να είναι:

- πλήρως εξοπλισμένες και έτοιμες για χρήση τους από τον οργανισμό
- μερικώς εξοπλισμένες
- μη εξοπλισμένες με όσα χρειάζονται για άμεση χρήση τους αλλά με ρεύμα και τηλεφωνική σύνδεση.

Μια αρκετά ενδιαφέρουσα στρατηγική λήψης αντιγράφων είναι αυτή της λήψης εικόνων των δίσκων (**disk image**) με κατάλληλο λογισμικό που υποστηρίζει, επίσης, και διαφορικό ή αυξητικό αντίγραφο ασφαλείας.

Σύγχρονες τάσεις και τεχνολογίες στην διαδικασία ανάκαμψης είναι η **Εικονικοποίηση**[3] **(Virtualization)** και το **Υπολογιστικό Νέφος** ή **Σύννεφο (Cloud Computing)**.

Με την χρήση Εικονικοποιημένων Διακομιστών (**Server Virtualization**) για παράδειγμα, αυξάνεται η ταχύτητα ανταπόκρισης σε επείγουσες καταστάσεις (ανάκαμψη):

- εύκολη μεταφορά τους,
- μειώνεται η ανάγκη Υλικού (Hardware) και χώρου τοποθέτησής τους
- μπορεί να συνεχίσει την λειτουργία του σχεδόν άμεσα, εάν προκύψει hardware πρόβλημα.

Το Υπολογιστικό Νέφος και ειδικά η **Αποθήκευση στο Νέφος (Cloud Storage)** προσφέρει αρκετά πλεονεκτήματα στον Σχεδιασμό Ανάκαμψης:

- μεγάλο αποθηκευτικό χώρο με χαμηλό κόστος,
- αυτοματοποιεί την διαδικασία Αντιγράφων Ασφαλείας (back-up),

[3] Περισσότερα για την Εικονικοποίηση αναφέρονται στο Κεφάλαιο 6.

- μειώνει την ανάγκη ύπαρξης διαφορετικών χώρων για την αποθήκευση των Αντιγράφων Ασφαλείας.

Σημαντικό θέμα που αφορά το Υπολογιστικό Νέφος είναι η ασφάλεια αποθήκευσης σε αυτό.

## 5.3 Ασφάλεια Λογισμικού

**5.3.1 Λογισμικό Κακόβουλης Χρήσης** (Malware) είναι το λογισμικό που μπορεί να προκαλέσει κάποιου είδους ζημιά στα συστήματα. Υπάρχουν άτομα αλλά και ομάδες ατόμων που χρησιμοποιούν προγράμματα ή εκμεταλλεύονται (*exploit*) κενά ασφαλείας εγκατεστημένων προγραμμάτων για διάφορους λόγους. Διασκέδαση, επίδειξη ικανοτήτων, οικονομικό όφελος, εκδίκηση αλλά και εκφοβισμό.

Αν και τα περισσότερα άτομα που χρησιμοποιούν το διαδίκτυο (internet) γνωρίζουν πως υπάρχουν προβλήματα ασφαλείας σ' αυτό δεν αντιλαμβάνονται το μέγεθος του κινδύνου που διατρέχουν. Η επίσκεψη μιας ιστοσελίδας με οδηγίες για Hacking, με πειρατικό λογισμικό, το άνοιγμα ενός περίεργου ηλεκτρονικού μηνύματος (email), το χτύπημα ενός συνδέσμου από περίεργη διαφήμιση, μια εφαρμογή για κινητό τηλέφωνο (smart phone) ακόμα και ένα δωρεάν διαθέσιμο πρόγραμμα μπορεί να περιέχει κακόβουλο λογισμικό και να προκαλέσει σοβαρά προβλήματα.

Υπάρχουν πολλά είδη κακόβουλου λογισμικού με γνωστότερες κατηγορίες τις εξής:

1. **Spyware:** σκοπό έχουν την συλλογή πληροφοριών και την αποστολή τους στον δημιουργό τους. Καταγράφουν τις δραστηριότητες σε σελίδες αλλά και ό,τι πληκτρολογεί (keylogger) ο χρήστης ακόμα και κωδικούς.
2. **Adware**: αυτά προβάλλουν ανεπιθύμητες διαφημίσεις και ενδεχομένως να καταγράφουν τις συνήθειες του χρήστη και να τις αποστέλλουν στον δημιουργό τους. Συνήθως είναι μέρος δωρεάν προγραμμάτων αλλά και πρόσθετων σε φυλλομετρητές.
3. **Trojan** (horse): αυτό που επιδιώκουν είναι να δώσουν άμεση πρόσβαση στον διαχειριστή τους στο σύστημα και τα αρχεία του. Η εγκατάστασή του γίνεται υπό την κάλυψη κάποιου χρήσιμου προγράμματος ή παιχνιδιού. Με την εκτέλεση του μολυσμένου αρχείου (του Δούρειου ίππου - trojan) το οποίο έχει μέσα του δυο προγράμματα, το χρήσιμο και το Trojan, εγκαθίστανται και τα δυο και το χρήσιμο εκτελείται κανονικά.
4. **Viruses**: ο προορισμός τους καθορίζεται από τον δημιουργό τους. Μπορεί να είναι ακίνδυνοι αλλά και επιβλαβής για συστήματα και χρήστες. Μεταδίδονται μέσω της εκτέλεσης των αρχείων στα οποία έχουν προσκολληθεί σε άλλα υγιή αρχεία.
5. **Worms**: μπορούν να στέλνουν προσωπικά δεδομένα στους δημιουργούς τους. Μεταδίδονται μέσω δικτύων και ηλεκτρονικών μηνυμάτων (emails) και επιβαρύνουν την κίνηση του δικτύου
6. **Backdoor**: με τις Κερκόπορτες ο δημιουργός τους αποκτά κανάλι επικοινωνίας με τον Η/Υ όπου εγκαταστάθηκε και μπορεί να εκτελέσει εντολές σε αυτόν όποτε θελήσει. Συνήθως εισχωρούν με την βοήθεια Trojan.
7. **Botnet**: είναι το δίκτυο από Bots, δηλαδή τους Η/Υ θύματα με το κακόβουλο λογισμικό. Η εγκατάσταση του λογισμικού γίνεται συνήθως από φυλλομετρητές, από Trojan και από συνημμένα ηλεκτρονικών μηνυμάτων (email attachments). Το δίκτυο των Η/Υ θυμάτων μπορεί και ελέγχεται κεντρικά μέσω πρωτοκόλλων όπως το IRC, HTTP και συχνά χρησιμοποιείται για επιθέσεις Άρνησης Υπηρεσιών (Denial of Services).

8. **Rootkit**: είναι ένα πολύ δύσκολα εντοπιζόμενο κακόβουλο λογισμικό που συνήθως καλύπτει άλλα κακόβουλα λογισμικά όπως τα Backdoors.

### 5.3.2 Λογισμικό Προστασίας από Κακόβουλο Λογισμικό (Antivirus).

Η χρήση των Η/Υ σε ολοένα και περισσότερες δραστηριότητες στο διαδίκτυο, η χρήση φορητών μέσων αποθήκευσης και οι συνεχώς αυξανόμενες απειλές σ' αυτό έχουν κάνει απαραίτητη τη χρήση προγραμμάτων προστασίας (antivirus) από κακόβουλα λογισμικά. Η προσβολή συστημάτων εντός ενός οργανισμού μπορεί να προκαλέσει προβλήματα στις Βασικές Αρχές ασφαλείας, τριάδα ΕΑΔ, Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα.

Αν και η απόλυτη προστασία είναι σχεδόν αδύνατο να επιτευχθεί, θα πρέπει να επιδιώκεται η καλύτερη δυνατή. Υπάρχουν πολλά προγράμματα που προσφέρουν ικανοποιητική προστασία και τα οποία με μικρό αντίτιμο, ως προς αυτά που προσφέρουν, μπορούν να εγκατασταθούν στα συστήματα. Η επιλογή των προγραμμάτων αυτών δεν θα πρέπει να γίνεται βάσει φημών από φίλους και γνωστούς, αλλά με κριτήρια, όπως τις δυνατότητες προστασίας που προσφέρει αλλά και τις δυνατότητες του συστήματος που θα εγκατασταθεί. Ενδεικτικά θα πρέπει να έχει τις εξής δυνατότητες:

- Ανίχνευση όλων των ειδών κακόβουλων λογισμικών
- Ανίχνευση συμπιεσμένων αρχείων
- Αυτόματη ανίχνευση USB συσκευών
- Προστασία των ηλεκτρονικών μηνυμάτων και άμεσων μηνυμάτων

Πέρα της επιλογής του κατάλληλου προγράμματος προστασίας θα πρέπει στη συνέχεια να γίνουν και οι σωστές ρυθμίσεις του:

- Αυτόματη ενημέρωση της βάσης του και του προγράμματος
- Ενεργοποίηση των δυνατοτήτων του προγράμματος προστασίας
- Τακτικό πλήρη έλεγχο του συστήματος
- Προστασία των ρυθμίσεων με κωδικό

**5.3.3 Ενημερώσεις (Updates) Λειτουργικών Συστημάτων και Εφαρμογών.** Είναι σύνηθες να υπάρχει σ' ένα Πληροφοριακό Σύστημα και λογισμικό που αναπτύσσεται εντός του οργανισμού για τις δικές του εξειδικευμένες ανάγκες. Το λογισμικό αυτό αλλά και οι ενημερώσεις του απαιτούν εντατικούς ελέγχους σε απομονωμένο περιβάλλον από το τμήμα για το οποίο προορίζεται, προκειμένου να προστατευτεί το Πληροφοριακό Σύστημα.

Εκτός του εσωτερικά αναπτυγμένου λογισμικού υπάρχει και λογισμικό του εμπορίου. Το λογισμικό αυτό, συνήθως, υπάρχει διαθέσιμο στις ιστοσελίδες των εταιριών που το παράγουν και αυτό διευκολύνει κακόβουλες ομάδες στο να μελετήσουν και να εντοπίσουν κενά ασφαλείας του, ώστε μέσω αυτών να επιτεθούν στους χρήστες του λογισμικού.

Ένα από τα συνηθέστερα προγράμματα που γίνεται στόχος επιθέσεων είναι οι φυλλομετρητές ιστοσελίδων (web browsers) και διάφορα πρόσθετα που χρησιμοποιούν αυτοί για προβολή βίντεο, παιχνίδια αλλά και για εκτέλεση web εφαρμογών. Οι εταιρείες παραγωγής λογισμικού εκδίδουν συχνά ενημερώσεις των προγραμμάτων τους, για να επιδιορθώσουν διάφορα προβλήματα, μεταξύ των οποίων και κενά ασφαλείας. Για διευκόλυνση έχουν ενσωματωμένο έλεγχο για ενημερώσεις και εγκατάστασή τους και μπορεί να ελεγχθεί εύκολα αυτό από τις ρυθμίσεις του κάθε προγράμματος.

Στόχος επιθέσεων γίνονται και τα Λειτουργικά Συστήματα. Επιβεβλημένος για την προστασία του είναι ο αυτόματος έλεγχος για ενημερώσεις του και η εφαρμογή τους σχεδόν σε όλα στα συστήματα. Στα κρίσιμα συστήματα πρώτα θα πρέπει να γίνεται έλεγχος για το πώς θα τα επηρεάσουν οι ενημερώσεις πριν εγκατασταθούν, προκειμένου να αποφευχθούν προβλήματα διαθεσιμότητάς τους.

Σημαντικότατος είναι και ο ρόλος των χρηστών στην έκθεση συστημάτων σε απειλές. **Επιβάλλεται** οι χρήστες να συνδέονται στα συστήματα με λογαριασμούς **περιορισμένων δικαιωμάτων** (τυπικού χρήστη – typical user). Σε περιπτώσεις συνδέσεως με πλήρη δικαιώματα (διαχειριστή – Administrator για Windows ή root για Linux) είναι ιδιαίτερα επικίνδυνη η προσβολή από κακόβουλο λογισμικό γιατί αυτό θα μπορεί να επηρεάσει πολύ σοβαρότερα ένα σύστημα από ότι εάν είχε γίνει σε απλού χρήστη σύνδεση.

### 5.3.4 Κρυπτογραφία (Cryptography).

Η κρυπτογραφία μελετά τρόπους εξασφάλισης της εμπιστευτικότητας στην επικοινωνία δυο πλευρών.

Χρήσιμη ορολογία στην κρυπτογραφία είναι η παρακάτω:

- **Κρυπτογράφηση** (Encryption): Η διαδικασία μετασχηματισμού του μηνύματος από το αρχικό μήνυμα στο τελικό μη αναγνώσιμο
- **Αποκρυπτογράφηση** (Decryption): η αντίστροφη διαδικασία της κρυπτογράφησης
- **Αρχικό κείμενο** (Plaintext): το αρχικό μήνυμα
- **Αλγόριθμος κρυπτογράφησης** (Cipher) : ο αλγόριθμος (ο τρόπος) με τον οποίο θα μετατραπεί το αρχικό μήνυμα σε μη αναγνώσιμο
- **Κρυπτογράφημα** (ciphertext): το τελικό μη αναγνώσιμο μήνυμα
- **Κλειδί** (key): είναι μια σειρά αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Για να υλοποιηθούν οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούνται μαθηματικά όπως: πρώτοι αριθμοί, ημίπρωτοι, παραγοντοποίηση κ.λπ.

Η κρυπτογραφία χρησιμοποιείται ευρύτατα σήμερα στην καθημερινότητα χωρίς να γίνεται αντιληπτό, σε ηλεκτρονικές συναλλαγές, κινητή τηλεφωνία αλλά και στα ασύρματα δίκτυα (Wifi).

Σε γενικές γραμμές αυτό που θέλουν να πετύχουν οι αλγόριθμοι κρυπτογράφησης μπορεί να περιγραφεί ως εξής: έστω πως υπάρχουν δύο φίλοι, ο Άκης και η Βούλα, οι οποίοι θέλουν να ανταλλάξουν μηνύματα με ασφάλεια (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το μετατρέψει με κάποιο κλειδί σε μη αναγνώσιμη από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να το ξεκλειδώσει και να διαβάσει το περιεχόμενό του.

Στη μοντέρνα κρυπτογραφία υπάρχουν δύο ειδών κρυπτογραφήσεις, **Συμμετρικού κλειδιού** (Symmetric key) και **Ασύμμετρου κλειδιού ή Δημοσίου κλειδιού** (Asymmetric key – Public key).

**Συμμετρικού κλειδιού** λέγονται αυτοί που χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση αλλά και για την αποκρυπτογράφηση. Θα πρέπει δηλαδή να γνωρίζει ο παραλήπτης το κλειδί που χρησιμοποίησε ο αποστολέας.

Γνωστοί συμμετρικοί αλγόριθμοι είναι: ο **AES** που χρησιμοποιείται σε πολλά ασύρματα δίκτυα και ο **Blowfish** που χρησιμοποιείται συχνά για κρυπτογράφηση κωδικών σε Βάσεις Δεδομένων αλλά και των κωδικών χρηστών του Linux στο /etc/password.

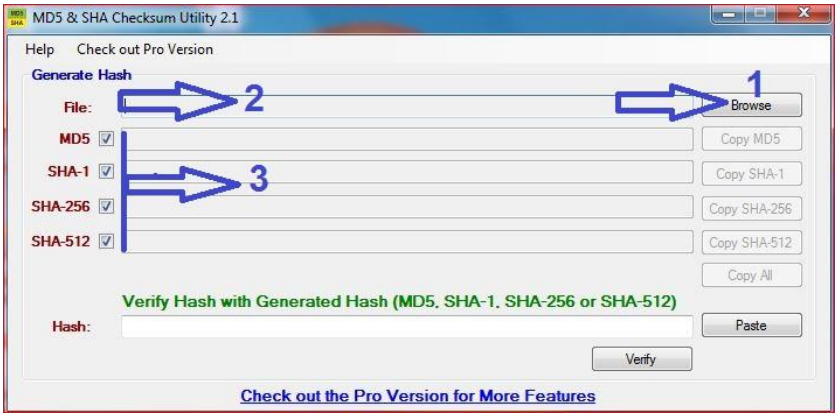
Στην **Ασύμμετρου κλειδιού ή Δημοσίου κλειδιού** υπάρχει ένα ζευγάρι κλειδιών που παράγονται ταυτόχρονα. Το ιδιωτικό κλειδί (private key) που το γνωρίζει μόνο ο ιδιοκτήτης του και το δημόσιο κλειδί (public key) που μπορούν να το γνωρίζουν όλοι, χωρίς να επηρεάζει αυτό σε τίποτα την ασφάλεια του ιδιοκτήτη του ζεύγους κλειδιών. Δεν είναι δυνατόν να υπολογίσει κάποιος το ιδιωτικό κλειδί κάποιου εάν γνωρίζει το δημόσιο κλειδί του.

**Παράδειγμα χρήσης Ασύμμετρου κλειδιού**: έστω πως ο Άκης θέλει να στείλει ένα μήνυμα στην Βούλα και έχει ο καθένας το δικό του ζευγάρι κλειδιών (ιδιωτικό, δημόσιο). Ο Άκης θα ετοιμάσει το μήνυμά του, θα χρησιμοποιήσει το **δημόσιο** κλειδί της Βούλας για να κρυπτογραφήσει το μήνυμά του και θα το στείλει στην Βούλα. Η Βούλα τώρα, για να το διαβάσει, θα πρέπει να χρησιμοποιήσει το **ιδιωτικό** της κλειδί.

Γνωστότερος αλγόριθμος κρυπτογράφησης Δημοσίου κλειδιού είναι ο RSA.

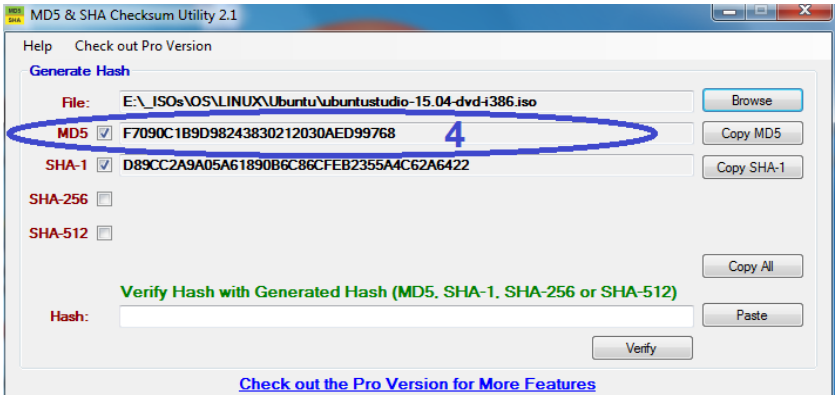
***Έλεγχος ακεραιότητας*** αρχείου. Ο έλεγχος του αν τροποποιήθηκε ένα αρχείο γίνεται με προγράμματα υπολογισμού και επιβεβαίωσης *Ελέγχου Αθροίσματος* (Checksum calculator-validator) ή Hash Generators. Γενικός τρόπος χρήσης τους είναι ο εξής:

**Δημιουργία (εύρεση) αθροίσματος ελέγχου (checksum):**




Εικόνα 5.2: Βήματα για δημιουργία checksum

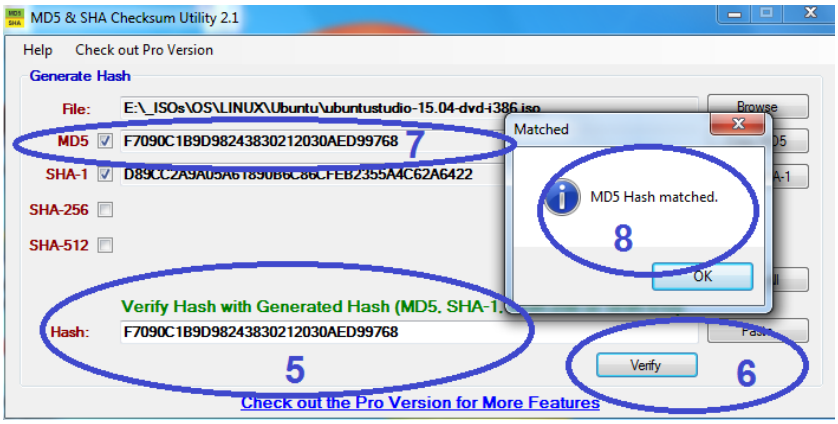
1. Από το σημείο 1 της εικόνας 5.2 γίνεται η επιλογή του αρχείου που θα υπολογιστεί το άθροισμα ελέγχου (checksum).
2. Στο σημείο 2 θα εμφανιστεί το όνομα αρχείο που επιλέχθηκε.
3. Στο σημείο 3 θα εμφανιστούν τα αθροίσματα ελέγχου σε MD5, SHA-1 κ.λπ. Αυτά είναι που χρειάζονται για τον έλεγχο ακεραιότητας.




Εικόνα 5.3: Το άθροισμα ελέγχου MD5

4. Στο σημείο 4 (εικ.5.3) υπάρχει το MD5 άθροισμα ελέγχου (MD5 checksum) του αρχείου που επιλέχθηκε. Αυτό το υπολογισμένο άθροισμα ελέγχου χρειάζεται για να ελεγχτεί η ακεραιότητα του αρχείου μελλοντικά.

**Επιβεβαίωση αθροίσματος ελέγχου (checksum):**




Εικόνα 5.4: Έλεγχος ακεραιότητας αρχείου με χρήση checksum MD5

Όταν θελήσει κάποιος να ελέγξει την ακεραιότητα του αρχείου θα κάνει τα εξής βήματα:

5. Σημείο 5 (εικ.5.4): αφού επαναλάβει τα βήματα 1, 2, 3 για να υπολογίσει το MD5 άθροισμα ελέγχου του αρχείου που έχει αυτός στον Η/Υ του, θα βάλει στην θέση 5 το MD5 άθροισμα ελέγχου που του στάλθηκε ή βρήκε στην ιστοσελίδα από όπου κατέβασε το αρχείο.
6. Σημείο 6: θα δώσει εντολή από το κουμπί *Verify* (επιβεβαίωσε) να συγκριθούν τα περιεχόμενα του σημείου 5 με αυτά του σημείου 7.
7. Θα εμφανιστεί το μήνυμα στο σημείο 8 που θα επιβεβαιώνει πως είναι ίδια (matched) αυτά τα δύο άρα δεν τροποποιήθηκε το αρχείο ή θα εμφανίσει μήνυμα πως δεν είναι ίδια το 5 με το 7 που σημαίνει πως κάτι έχει αλλάξει στο αρχικό αρχείο.

Από το παραπάνω παράδειγμα προκύπτει το συμπέρασμα πως **είναι σημαντικότατη η προστασία του αρχικού αθροίσματος ελέγχου** από **τροποποιήσεις**.

**Η Ψηφιακή υπογραφή** χρησιμοποιεί κρυπτογραφία δημοσίου κλειδιού και πιστοποιεί πως δεν τροποποιήθηκε το μήνυμα του αποστολέα. Την αυθεντικότητα του αποστολέα, το ποιος είναι στην πραγματικότητα, μπορεί να την πιστοποιήσει μια **Αρχή Πιστοποίησης** η οποία ελέγχει και πιστοποιεί την ταυτότητα και το δημόσιο κλειδί του με **Ψηφιακό Πιστοποιητικό**. Για παράδειγμα, το Πανελλήνιο Σχολικό Δίκτυο (ΠΣΔ) έχει τέτοια Αρχή Πιστοποίησης στη σελίδα http://ca.sch.gr που πιστοποιεί την ταυτότητα των εκπαιδευτικών. Αυτό μπορεί και το κάνει γιατί έχει τα απαραίτητα στοιχεία κάθε εκπαιδευτικού, στοιχεία αστυνομικής ταυτότητας αλλά και τη διεύθυνση ηλεκτρονικού ταχυδρομείο τους στο ΠΣΔ.

**Η Κρυπτογράφηση δίσκων, κατατμήσεων** (partitions) και **αρχείων** γίνεται για να εξασφαλιστεί η εμπιστευτικότητα του περιεχομένου τους. Πως δεν θα μπορέσει να διαβαστεί δηλαδή από τρίτους, για παράδειγμα, σε περίπτωση κλοπής. Γι' αυτό χρησιμοποιείται συχνά σε φορητούς υπολογιστές αλλά και φορητές συσκευές αποθήκευσης. Προγράμματα κρυπτογράφησης υπάρχουν συνήθως ενσωματωμένα στα Λειτουργικά Συστήματα αλλά υπάρχουν και πολλά προγράμματα τρίτων. Από τη στιγμή που θα γίνει η κρυπτογράφηση ο μόνος τρόπος για να μπορέσουν να διαβαστούν τα δεδομένα είναι να γνωρίζει κάποιος τον κωδικό που χρησιμοποιήθηκε κατά την κρυπτογράφηση.

## 5.4 Ασφάλεια Δικτύου

Όπως ένα κτίριο προστατεύεται με φρουρούς και συναγερμούς, έτσι και το δίκτυο ενός οργανισμού χρειάζεται προστασία από μη εξουσιοδοτημένα άτομα. Χρειάζεται διάφορους φραγμούς, προκειμένου να προστατευτούν οι πληροφορίες που υπάρχουν σ' αυτό από εσωτερικές και εξωτερικές απειλές. Με αυτόν τον τρόπο συμβάλλει και στην αξιοπιστία του οργανισμού που ανήκει. Σημαντικά τμήματά της για την ασφάλεια και την σωστή λειτουργία του δικτύου είναι:

**5.4.1 Τείχος Προστασίας (Firewall),** μπορεί να είναι λογισμικό ή υλικό και σκοπός του είναι να ελέγχει την κίνηση μεταξύ των δικτύων που συνδέει και ανάλογα με τις λίστες ελέγχου πρόσβασης (ACL) που έχει να την επιτρέπει ή να την απορρίπτει. Μπορεί για παράδειγμα, να απαγορεύει την πρόσβαση των συστημάτων από το τμήμα προσωπικού του οργανισμού στα συστήματα του οικονομικού τμήματος ή να επιτρέπει κίνηση προς ένα σύστημα μόνο για συγκεκριμένη υπηρεσία όπως της εξυπηρέτησης ιστοσελίδων.

**5.4.2 Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network – VPN)** είναι μια υπηρεσία πελάτη/εξυπηρετητή (client/server) που επιτρέπει την επικοινωνία συστημάτων με ασφάλεια μέσω ενός εικονικού τούνελ. Για παράδειγμα, θα μπορούσε ένα μέλος του οργανισμού να βρίσκεται σε διαφορετικό κράτος και με την χρήση ενός προγράμματος πελάτη VPN που θα τρέξει στον φορητό του να συνδεθεί στον εξυπηρετητή VPN του οργανισμού και αυτός να του δώσει πρόσβαση στο εσωτερικό δίκτυο σαν να βρισκότανε εντός του δικτύου. Θα μπορεί να χρησιμοποιεί δηλαδή, τους πόρους του κεντρικού δικτύου του οργανισμού όπως: εκτυπωτές, κοινόχρηστους φακέλους, βάσεις δεδομένων κ.λπ. Πρωτόκολλα που χρησιμοποιούνται εδώ είναι τα PPTP, L2TP, GRE, και IPSec.

**5.4.3 Σύστημα Ανίχνευσης Εισβολής (Intrusion Detection System – IDS),** με αυτό παρακολουθείται και αναλύεται ό,τι συμβαίνει στο δίκτυο του οργανισμού. Σκοπός του είναι, να εντοπίζει προσπάθειες εισβολής μη εξουσιοδοτημένων ατόμων σε συστήματα, καθώς κάτι

τέτοιο θα έβαζε σε κίνδυνο παραβίαση κάποιας αρχής από την τριάδα των Βασικών Αρχών (ΕΑΔ). Για να παρακολουθεί την κίνηση του δικτύου το IDS, θα πρέπει να διοχετεύεται σ' αυτό η κίνηση του δικτύου με κάποιον τρόπο. Αν υπάρχει συσκευή HUB τότε είναι απλό, διαφορετικά γίνεται με Μεταγωγείς Δικτύου (Network Switches) που υποστηρίζουν τέτοια λειτουργία σε κάποια πόρτα (port) τους. Ανάλογα με την εταιρεία κατασκευής, η πόρτα αυτή του Μεταγωγέα ή υποστήριξη τέτοιος δυνατότητας από τον Μεταγωγέα μπορεί να ονομάζεται: Port Mirroring, Monitoring Port, Spanning Port και SPAN port. Αυτές οι πόρτες είναι συνήθως μόνο παθητικές, δηλαδή μόνο λαμβάνουν δεδομένα. Όταν το IDS εντοπίζει ύποπτη κίνηση στο δίκτυο, μπορεί και ενημερώνει τον υπεύθυνο ασφαλείας του δικτύου ή να κάνει ενέργειες για την διακοπή των ύποπτων κινήσεων.

## 5.5 Φυσική Ασφάλεια

Φυσική ασφάλεια είναι η προστασία του χώρου ενός οργανισμού και του εξοπλισμού του από απειλές όπως φωτιά, κλοπή κ.λπ. Είναι εξίσου σημαντική με τα άλλα μέτρα ασφαλείας γιατί μέσα στον χώρο υπάρχει η υποδομή του Πληροφοριακού Συστήματος.

Θα πρέπει να εξασφαλίζονται οι απαιτούμενες περιβαλλοντολογικές συνθήκες όπως υγρασία, θερμοκρασία και σκόνη.

Να υπάρχει συναγερμός για παραβιάσεις αλλά και για έκτακτες περιπτώσεις, όπως φωτιάς.

Ο έλεγχος φυσικής πρόσβασης στο κτίριο μπορεί να γίνεται από φρουρούς, κάμερες, συσκευές βιομετρικών ελέγχων (δακτυλικό αποτύπωμα, ίριδα ματιού, χαρακτηριστικών προσώπου, φωνής) και μαγνητικών καρτών.

Ο έλεγχος επισκεπτών είναι εξίσου σημαντικός, καθώς μπορούν να προκαλέσουν εύκολα προβλήματα, γι' αυτό δεν θα πρέπει να χρησιμοποιούν συσκευές USB εντός του οργανισμού, ούτε να έχουν πρόσβαση στο δίκτυο του οργανισμού.

## Ερωτήσεις

**Ενότητας 5.1**

1. Ποιο είναι το αντικείμενο της Ασφάλειας Πληροφοριακών Συστημάτων;

**Ενότητας 5.2**

2. Ποιες είναι οι Βασικές Αρχές της Ασφάλειας Πληροφοριακών Συστημάτων;
3. Τι είναι ο Έλεγχος Πρόσβασης; Δώστε δυο παραδείγματα.
4. Τι είναι τα Αρχεία Καταγραφής (Logfiles); Δώστε ένα παράδειγμα χρήσης τους.
5. Τι είναι η Πιστοποίηση Ταυτότητας (Authentication); Ποιος είναι ο συνηθέστερος τρόπος επίτευξής του;
6. Τι είναι το Active Directory και το Ldap;
7. Ποιος είναι ο σκοπός της Διαχείρισης Κινδύνου;
8. Τι προσδιορίζει η Αξιολόγηση Κινδύνου;
9. Τι σημαίνει Απειλή και Ευπάθεια σε ένα Πληροφοριακό Σύστημα; Δώστε δυο παραδείγματα απειλής-ευπάθειας.
10. Τι είναι η Πολιτική Ασφαλείας και από τι επηρεάζεται η εφαρμογή της;
11. Τι είναι Επιχειρησιακή Συνέχεια και πως επηρεάζεται από την Επαναφορά από Καταστροφή;

12. Γιατί είναι απαραίτητα τα Αντίγραφα Ασφαλείας; Πως λέγεται η αντίστροφη διαδικασία;
13. Περιγράψτε την διαδικασία ενός τρόπου λήψης Αντιγράφων Ασφαλείας.

**Ενότητας 5.3**

14. Τι είναι το λογισμικό κακόβουλης χρήσης και πως εισχωρεί στα συστήματα Η/Υ;
15. Περιγράψτε τρία είδη κακόβουλου λογισμικού.
16. Τι δυνατότητες πρέπει να έχει ένα πρόγραμμα προστασίας από κακόβουλο λογισμικό (malware);
17. Ποιες ρυθμίσεις θα πρέπει να εφαρμόζονται στα προγράμματα προστασίας από κακόβουλο λογισμικό;
18. Γιατί είναι απαραίτητος ο έλεγχος για ενημερώσεις και εφαρμογή τους σε προγράμματα και λειτουργικά συστήματα;
19. Πως γίνεται ο έλεγχος ενημερώσεων για εφαρμογές και λειτουργικά συστήματα;
20. Περιγράψτε την διαδικασία αποστολή κρυπτογραφημένου μηνύματος με την χρήση Δημοσίου Κλειδιού.
21. Πως μπορεί να ελεγχθεί η ακεραιότητα (αν τροποποιήθηκε) ενός αρχείου;
22. Για ποιον λόγο χρησιμοποιείται η Ψηφιακή Υπογραφή και η Αρχή Πιστοποίησης;
23. Πότε χρειάζεται η κρυπτογράφηση εσωτερικών ή εξωτερικών δίσκων ενός συστήματος;

**Ενότητας 5.4**

24. Σε τι χρησιμεύει το Τείχος Προστασίας (firewall);
25. Περιγράψτε με παράδειγμα τα οφέλη από την χρήση Εικονικού Ιδιωτικού Δικτύου (VPN).

**Ενότητας 5.5**

26. Γιατί θα πρέπει να απαγορεύεται η χρήση USB δίσκων και η πρόσβαση στο εσωτερικό δίκτυο ενός οργανισμού από επισκέπτες;

## Δραστηριότητες

*Εικονικές Μηχανές Linux με προεγκατεστημένο το απαιτούμενο λογισμικό για τις δραστηριότητες υπάρχει στην ιστοσελίδα http://blogs.sch.gr/virtualization*

**Ενότητας 5.1**

1. Αναζητήστε πληροφορίες για τη συμβολή του Άλαν Τούριγκ στο χώρο της Πληροφορικής και δημιουργήστε μια παρουσίασή τους.
2. Βρείτε πληροφορίες για συγγενικά γνωστικά πεδία της Ασφάλειας Πληροφοριακών Συστημάτων και συζητήστε γι’ αυτά στην τάξη σας,.
3. Εντοπίστε ελληνικές ιστοσελίδες με πληροφορίες για το ηλεκτρονικό έγκλημα στην Ελλάδα και συζητήστε στην τάξη σας για τα δυο πιο διαδεδομένα είδη του.

**Ενότητας 5.2**

4. Σε ΛΣ του εργαστηρίου να δοθούν δικαιώματα χρήσης ενός φακέλου, ενός αρχείου και ενός εκτυπωτή σε άλλους χρήστες.
5. Να αναζητηθεί η ώρα σύνδεσης ενός χρήστη στα αρχεία καταγραφής (log files):
   α) των Windows (Καταγραφέα συμβάντων- Δεξί κλικ στον *Υπολογιστή μου/Διαχείριση*) και

β) σε Linux: *sudo cat /var/log/auth.log* ή Μενού *Εφαρμογές/Εργαλεία Συστήματος/Καταγραφέας του συστήματος*.

6. Να δημιουργήσετε απλό λογαριασμό χρήστη σε περιβάλλον Windows και Linux του εργαστηρίου σας και να δώσετε για κωδικό πρόσβασης μια φράση της επιλογής σας με τουλάχιστον 8 χαρακτήρες (πχ. *DenExo@ploPassword45*)
7. Να δημιουργήσετε Οργανική Μονάδα στο Active Directory, να προσθέσετε χρήστες και να τους παραχωρήσετε δικαιώματα σε διάφορους πόρους.
8. Να χρησιμοποιηθεί το εσωτερικό πρόγραμμα απ' το περιβάλλον Windows και Linux, για να γίνει λήψη αντιγράφων ασφαλείας του προσωπικού φακέλου ενός χρήστη. Μετά τη λήψη αντιγράφου ασφαλείας, να γίνει δοκιμαστική επαναφορά από το αντίγραφο ασφαλείας σε διαφορετικό φάκελο.

**Ενότητας 5.3**

9. Να χρησιμοποιηθούν προγράμματα προστασίας από κακόβουλο λογισμικό (antivirus) για να ελεγχθούν τα δοκιμαστικά αρχεία ιών (μη επικίνδυνων) από την ιστοσελίδα *http://www.eicar.org/85-0-Download.html* και να γίνουν οι προτεινόμενες ρυθμίσεις των προγραμμάτων αυτών.
10. Σε περιβάλλον Windows να ελεγχθούν χειροκίνητα για ενημερώσεις: ένας φυλλομετρητής, ο flash player και η java. Στη συνέχεια, να ρυθμιστούν για αυτόματο έλεγχο και κατέβασμα ή εγκατάστασή τους. Να γίνουν ανάλογες ενέργειες και σε Linux περιβάλλον.
11. Να γραφούν και αποθηκευτούν σε ένα απλό αρχείο κειμένου (keimeno1.txt) οι λέξεις «θα έρθω αύριο». Στη συνέχεια να γίνουν τα παρακάτω:
    1) να υπολογιστεί το MD5 checksum του και να αποθηκευτεί σε άλλο αρχείο (md5.txt).
    2) να προστεθεί στην αρχή του αρχικού κειμένου η λέξη «δε» και να αποθηκευτεί στο ίδιο αρχείο.
    3) να υπολογιστεί το νέο MD5 checksum του και να συγκριθεί με το αρχικό checksum (που βρίσκεται στο md5.txt).
12. Χρησιμοποιήστε σε έγγραφο μια ψηφιακή υπογραφή σας, την οποία θα δημιουργήσετε:
    α) τοπικά: στο Word πρώτα, από το μενού Προετοιμασία/Προσθήκη Ψηφιακής Υπογραφής/Δημιουργία του δικού σας, και στο OpenOffice μετά (θα υπάρχει αυτή από το Word) και
    β) σε ιστοσελίδα (π.χ. της Comodo.com)
13. Κρυπτογραφήστε ένα αρχείο σε περιβάλλον:
    1) Windows (Δεξί Κλικ / Ιδιότητες / Για προχωρημένους)
    2) Linux (πχ σε Ubuntu με δεξί κλικ σε αρχείο και επιλογή *Κρυπτογράφηση*, εφόσον υπάρχει η εφαρμογή Seahorse και αφού δημιουργηθεί σ' αυτό πρώτα PGP Key)

**Ενότητας 5.4**

14. Εξερευνήστε και συζητήστε για τις ρυθμίσεις προγράμματος Τείχους Προστασίας σε Windows (ενσωματωμένο) και Linux (πχ το gufw).
15. Συνδεθείτε στον τοπικό VPN server του σχολικού εργαστηρίου.

*Όλες οι εικόνες του κεφαλαίου 5 είναι του Παναγιωτίδη Σωτήριου*

# 6. Ειδικά Θέματα

Στο κεφάλαιο αυτό παρουσιάζονται οι βασικές γνώσεις για την Εικονικοποίηση (Virtualization) και τις Εικονικές Μηχανές (Virtual Machines), μια τεχνολογία ιδιαίτερα διαδεδομένη στο χώρο της Πληροφορικής τα τελευταία χρόνια.

**Διδακτικοί Στόχοι**

Στο κεφάλαιο αυτό θα μάθετε:

- τα οφέλη από τη χρήση τεχνολογίας Εικονικοποίησης,
- να εγκαθιστάτε προγράμματα Επόπτη Εικονικοποίησης (Virtualization Hypervisor)
- να δημιουργείτε Εικονικές Μηχανές,
- να εγκαθιστάτε λειτουργικά συστήματα σε Εικονικές Μηχανές,
- να μεταφέρετε Εικονικές Μηχανές σε άλλους υπολογιστές.

**Διδακτικές Ενότητες**

6.1 Εικονικές Μηχανές

## 6.1 Εικονικές Μηχανές

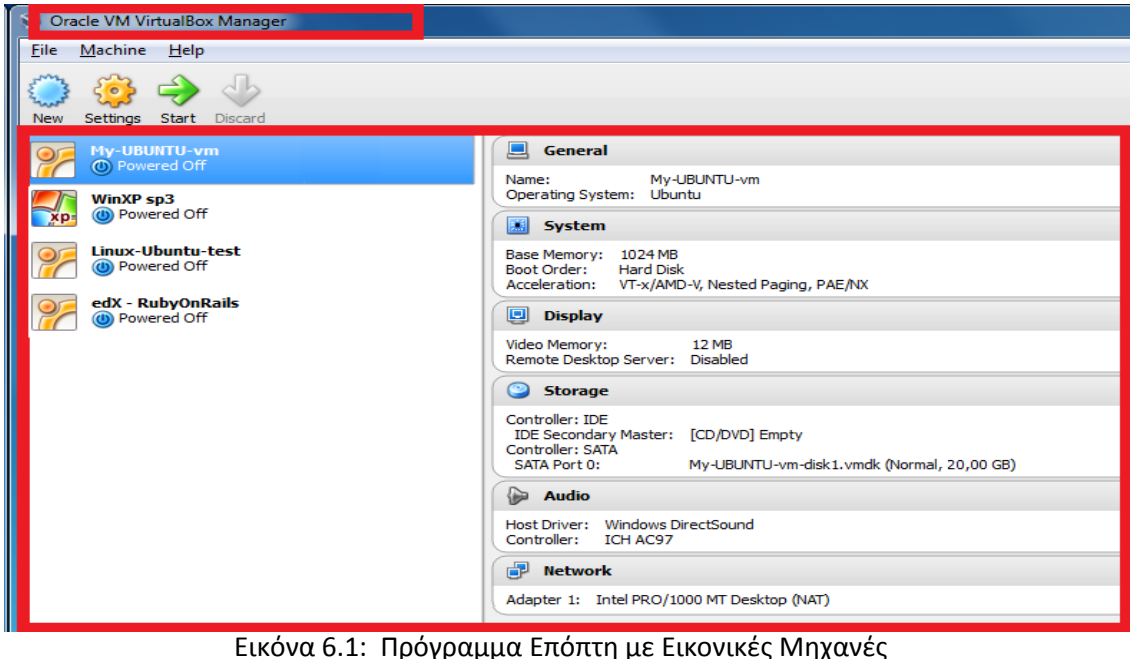
**Τι είναι μια Εικονική Μηχανή (Virtual Machine).** Είναι ένας εικονικός υπολογιστής, ένας υπολογιστής πρόγραμμα που μπορεί όμως και εκτελεί ότι και ένας πραγματικός υπολογιστής, να έχει δηλαδή δικό του Λειτουργικό Σύστημα και προγράμματα.

Η διαδικασία δημιουργίας εικονικών μηχανών λέγεται **Εικονικοποίηση[4] (virtualization).**

**Πως δημιουργείται μια εικονική μηχανή.** Για να δημιουργηθεί μια εικονική μηχανή χρειάζεται ένα πρόγραμμα **Επόπτη (Hypervisor)**. Από την στιγμή που θα εγκατασταθεί ένα τέτοιο πρόγραμμα μπορούν να δημιουργηθούν όσες εικονικές μηχανές (υπολογιστές) θέλει ο χειριστής του. Κάθε μηχανή που θα φτιάχνει θα είναι ένας φάκελος στον φυσικό υπολογιστή με λίγα αρχεία *(Εικόνα 6.2)*. Γνωστά δωρεάν προγράμματα Επόπτες είναι τα: *VirtualBox* της Oracle και *VMware Player* της VMware για ΛΣ Windows και Linux, το *Parallels* της εταιρίας Parallels και το *Fusion* της VMware για ΛΣ MacOS X, και τα *VirtualPC* και *Hyper-V* της Microsoft μόνο για Windows. ***Οδηγίες με εικόνες για τη δημιουργία εικονικής μηχανής και εγκατάστασης λειτουργικού συστήματος υπάρχουν στο Παράρτημα του κεφαλαίου 6***.

**Με τι υλικό (hardware) λειτουργεί μια εικονική μηχανή.** Κάθε μηχανή για να λειτουργήσει χρειάζεται πόρους όπως μνήμη, επεξεργαστή και σκληρό δίσκο. Αυτούς τους βρίσκει στον υπολογιστή που την φιλοξενεί. Η ρύθμιση των πόρων που θα της διατεθούν γίνεται από το πρόγραμμα Επόπτη, τα Mb φυσικής μνήμης RAM, το ποσοστό ισχύος της φυσικής ΚΜΕ και τα Gb χώρου του φυσικού σκληρού δίσκου που θα μπορεί να χρησιμοποιεί. Οι ρυθμίσεις αυτές μπορούν να αλλάξουν όποτε χρειαστεί.

Από το σημείο δημιουργίας της και μετά λειτουργεί όπως ένας κανονικός καινούργιος υπολογιστής αλλά μέσα σε παράθυρο. Μπορεί να εγκατασταθεί όποιο Λειτουργικό Σύστημα θέλει ο χειριστής του με τον τρόπο που θα το έκανε και σε φυσικό υπολογιστή από κανονικό CD ή USB stick αλλά και από αρχείο .ISO (εικόνα CD).




Εικόνα 6.1: Πρόγραμμα Επόπτη με Εικονικές Μηχανές

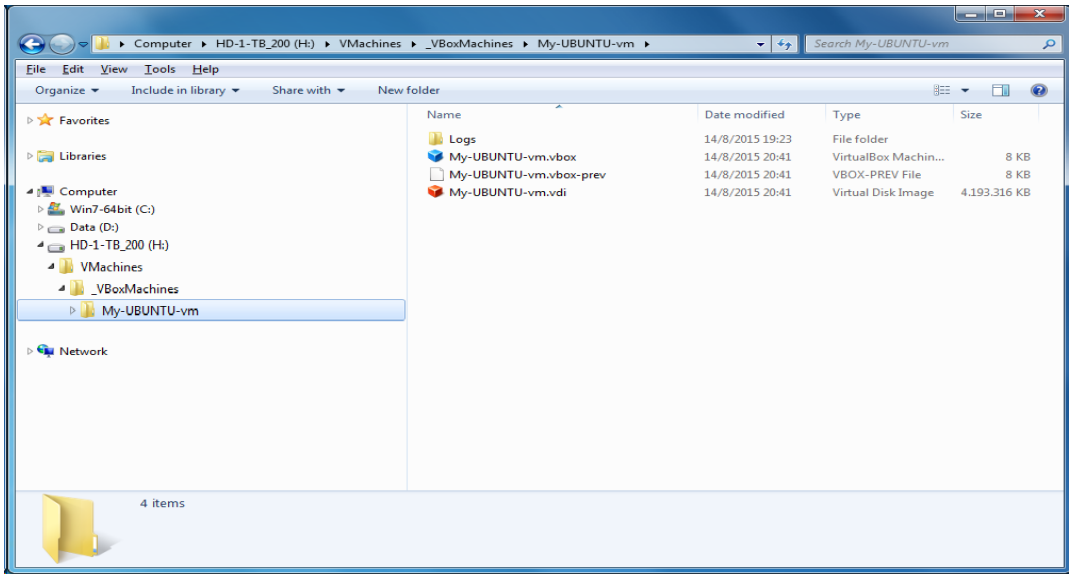
[4] Εικονικοποίηση και όχι εικονοποίηση επειδή φτιάχνει κάτι εικονικό και όχι εικόνες

Στην εικ. *6.1* φαίνεται ο Επόπτης του VirtualBox και ο συγκεκριμένος έχει στην διάθεσή του τέσσερις εικονικές μηχανές με λειτουργικά συστήματα. Κάθε μηχανή έχει τις δικές της ρυθμίσεις μνήμης RAM, ΚΜΕ (CPU) και σκληρού δίσκου. Εάν ο υπολογιστής που τις φιλοξενεί **(Host)** έχει αρκετούς πόρους τότε είναι δυνατόν να εκτελεστούν πολλές εικονικές μηχανές **(Guests)** ταυτόχρονα.

Η λειτουργία κάθε εικονικής μηχανής είναι απομονωμένη από των υπολοίπων. Αν περάσει δηλαδή κάποιο κακόβουλο λογισμικό σε έναν από αυτούς αυτό δεν θα επηρεάσει άλλες μηχανές ούτε τον υπολογιστή που την φιλοξενεί.

**Φορητότητα και Αντίγραφα ασφαλείας.** Όταν δημιουργηθεί μια εικονική μηχανή, θα είναι πλέον ένας φάκελος του φυσικού υπολογιστή με λίγα αρχεία μέσα σ' αυτόν, του εικονικού δίσκου και του αρχείου με τις επιλεγμένες ρυθμίσεις. Όπως και στους φυσικούς δίσκους, ανάλογα με το Λειτουργικό Σύστημα που θα εγκατασταθεί αλλά και με τα προγράμματα που θα εγκατασταθούν σε αυτόν, θα αυξάνονται και οι απαιτήσεις σε χώρο του εικονικού δίσκου.

Στην εικ. 6.2 φαίνεται ο φάκελος αποθήκευσης μιας εικονικής μηχανής. Το αρχείο ρυθμίσεων (.vbox) έχει μέγεθος 8Kb και ο εικονικός δίσκος (.vdi) στον οποίο περιέχονται το ΛΣ, οι εφαρμογές και τα αρχεία των χρηστών του, καταλαμβάνουν περίπου 4 Gb. Εάν αυτός ο



Εικόνα 6.2 Περιεχόμενα φακέλου εγκαταστημένης Εικονικής Μηχανή

φάκελος μεταφερθεί σε άλλο υπολογιστή, οπουδήποτε και αν είναι αυτός, και με οποιοδήποτε Λειτουργικό Σύστημα, στον οποίο όμως υπάρχει το πρόγραμμα Επόπτη, τότε θα μπορέσει να λειτουργήσει άμεσα.

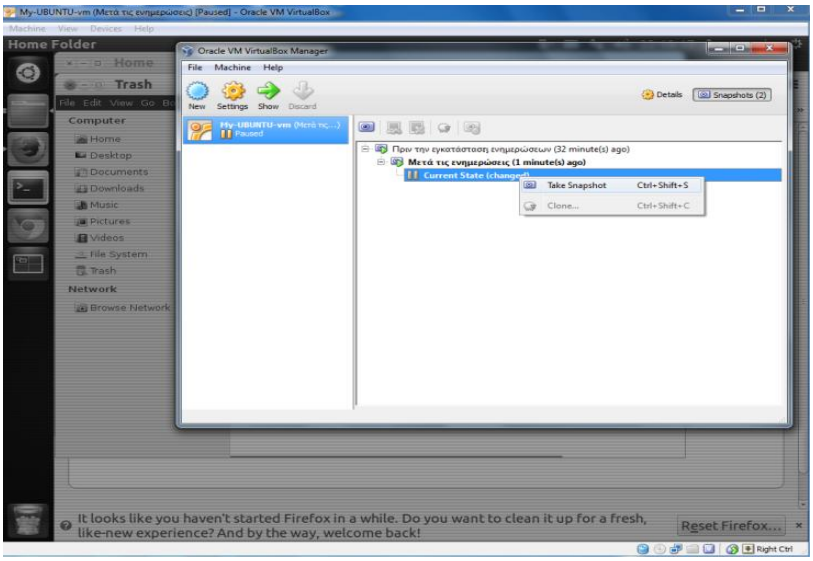
Αυτό μπορεί γίνει εκμεταλλεύσιμο, από ιδιώτες και επιχειρήσεις, σε καταστάσεις όπως, επαναφοράς από καταστροφή, γιατί δίνει τη δυνατότητα ένας διακομιστής (Server) εντός μικρού χρονικού διαστήματος να προσφέρει πάλι υπηρεσίες. Για παράδειγμα, εάν χαλάσει ο φυσικός σκληρός δίσκος ή ΚΜΕ ή μητρική κάρτα, τα μόνα που χρειάζονται για να επαναλειτουργήσει ο διακομιστής είναι: το **πρόσφατο αντίγραφο** της εικονικής μηχανής και ένας νέος υπολογιστής με το πρόγραμμα Επόπτη. Δεν χρειάζεται να έχει ίδια ΚΜΕ, μητρική, RAM. Δεν την επηρεάζει η χρήση διαφορετικού υλικού στο αν θα μπορέσει να λειτουργήσει,

μπορεί όμως να επηρεάσει τις επιδόσεις της εάν έχει διαθέσιμη λιγότερη μνήμη ή αριθμό πυρήνων ΚΜΕ.

Ορισμένα προγράμματα Επόπτες, όπως το VirtualBox της Oracle, προσφέρουν τη λειτουργία Στιγμιότυπα (Snapshots) (εικ. 6.3). Αυτή η λειτουργία, αποθηκεύει την κατάσταση της μηχανής την εκείνη τη χρονική στιγμή και στην οποία μπορεί να επανέλθει (εικ. 6.4) ο χειριστής όποτε θελήσει.

**Διαδικασία λήψης Στιγμιότυπου**

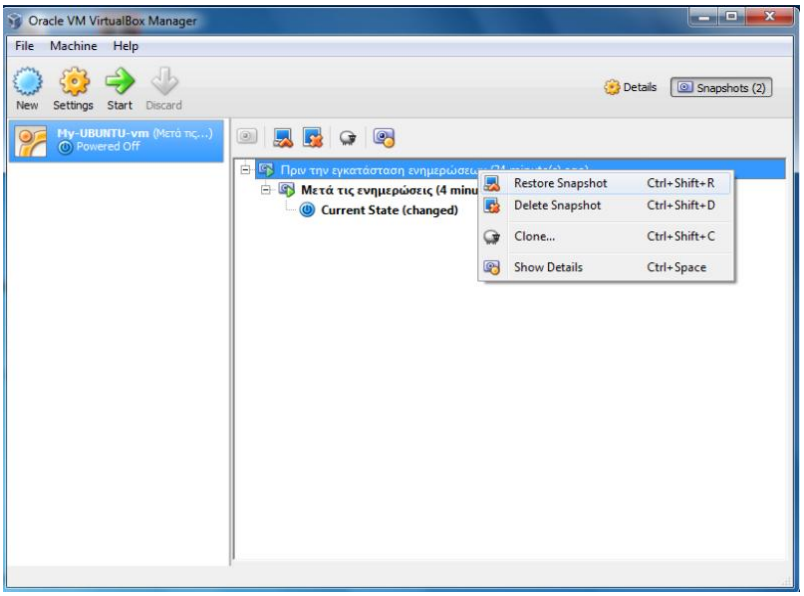
Κάνοντας δεξί κλικ στο *Current State* του βασικού παραθύρου του Επόπτη δίνεται η δυνατότητα επιλογής λήψης Στιγμιότυπου (*Take snapshot*)




Εικόνα 6.3 Λήψη στιγμιότυπου

**Διαδικασία επαναφοράς Στιγμιότυπου**

Στο βασικό παραθύρο του Επόπτη φαίνονται τα Στιγμιότυπα που έχουν παρθεί. Με δεξί κλικ πάνω στο Στιγμιότυπο δίνεται η επιλογή επαναφοράς του (restore *snapshot*) ή διαγραφής του (delete snapshot)




Εικόνα 6.4 Επαναφορά στιγμιότυπου

**Επισημάνσεις:**

- Υπάρχουν εφαρμογές οι οποίες **μπορούν να μετατρέψουν (convert) έναν φυσικό υπολογιστή σε εικονική μηχανή** (VMware vCenter Converter Standalone) χωρίς να επηρεάσουν τη λειτουργία του φυσικού υπολογιστή.

- Οι **άδειες χρήσης** λειτουργικών συστημάτων και προγραμμάτων σε εικονικές μηχανές ακολουθούν τους νομικούς κανόνες που ισχύουν και στους φυσικούς υπολογιστές

- Κατά τη χρήση των προγραμμάτων **Vmware Player** και **VirtualBox** ενδέχεται να παρουσιαστούν προβλήματα στην ανάλυση οθόνης (640x480 ή 800x600) της Εικονικής Μηχανής ή να εγκλωβιστεί ο δείκτης ποντικιού μέσα στο παράθυρο της Εικονικής Μηχανής. Λύσεις σε αυτά και άλλα προβλήματα λύνονται συνήθως με την εγκατάσταση των παρακάτω πρόσθετων <u>όταν είναι ενεργή</u> μια Εικονική Μηχανή:

  - στο **VirtualBox,** μενού **Devices / Install Guest Additions**

  - στο **Vmware Player,** μενού **Manage / Install VMware Tools**

  Για τον απεγκλωβισμό του δείκτη ποντικιού μπορεί να χρησιμοποιηθεί χωρίς την εγκατάσταση των παραπάνω προγραμμάτων η εξής λύση:

  - στο **Vmware Player** να πατηθεί ταυτόχρονα το αριστερό CTRL+ALT

  - στο **VirtualBox** χρειάζεται το δεξί CTRL.

- <u>Σε περίπτωση αλλαγής Επόπτη</u>:
  1. πριν την αλλαγή Επόπτη συνίσταται η απεγκατάσταση πρώτα του παλιού πρόσθετου προγράμματος (Guest Additions ή VMware Tools) του Επόπτη
  2. μετά γίνεται η αλλαγή Επόπτη (πχ. χρήση του εικονικού δίσκου από διαφορετικό Επόπτη)
  3. εγκατάσταση του νέου πρόσθετου (Guest Additions ή VMware Tools).

## 6.2 Ερωτήσεις

1. Τι λέγεται εικονική μηχανή;
2. Ποιος είναι ο ρόλος του προγράμματος Επόπτη Εικονικοποίησης;
3. Γιατί μπορεί να εκτελεστεί μια εικονική μηχανή σε διαφορετικό υπολογιστή από αυτόν στον οποίο δημιουργήθηκε;
4. Περιγράψτε έναν τρόπο λήψης αντιγράφου ασφαλείας μιας εικονικής μηχανής.
5. Από τι εξαρτάται ο αριθμός των εικονικών μηχανών που μπορούν να εκτελεστούν ταυτόχρονα σε ένα φυσικό υπολογιστή;
6. Αναζητήστε στο διαδίκτυο περιπτώσεις στις οποίες είναι χρήσιμη η μετατροπή ενός φυσικού υπολογιστή σε Εικονική Μηχανή, παρουσιάστε τες και συζητήστε τες στην τάξη σας

## 6.3 Δραστηριότητες

1. Να κατεβάσετε σε υπολογιστή του εργαστηρίου τα δωρεάν προγράμματα επόπτες VirtualBox και Vmware Player και να δημιουργήσετε με κάθε επόπτη δυο εικονικές μηχανές χωρίς λειτουργικά συστήματα.
2. Να εγκατασταθεί Λειτουργικό Σύστημα Linux σε εικονική συσκευή από:
   α) κανονικό CD/DVD
   β) εικόνα CD (αρχείο .iso) (CD image) που θα κατεβάσετε από ιστοσελίδα όποιας διανομής Linux επιθυμείτε.
   γ) να τεθεί ο εικονικός δίσκος του ΛΣ που εγκαταστάθηκε σε κατάσταση *Immutable,* εάν υποστηρίζεται αυτό από το πρόγραμμα Επόπτη.
3. Να μεταφέρεται σε διαφορετικό υπολογιστή μια υπάρχουσα εικονική μηχανή και να την εκτελέσετε.
4. Μετατρέψτε έναν φυσικό υπολογιστή του σχολικού εργαστηρίου σε Εικονική Μηχανή με την εφαρμογή VMware vCenter Converter Standalone.

# Παράρτημα 1. Ενώσεις, Οργανισμοί και Πρότυπα

Το παράρτημα αυτό αναφέρεται στο κεφάλαιο 5 και περιέχει ιστοσελίδες Ενώσεων και Οργανισμών - Διεθνή πρότυπα και Πιστοποιήσεις για επαγγελματίες στο χώρο της Ασφάλειας Πληροφοριών

**Ιστοσελίδες Ενώσεων και Οργανισμών**

| | |
|---|---|
| http://cert.sch.gr | - Υπηρεσία Αντιμετώπισης Περιστατικών Ασφαλείας ΠΣΔ |
| http://cert.grnet.gr | - Υπηρεσία Αντιμετώπισης Περιστατικών Ασφαλείας ΕΔΕΤ |
| http://www.enisa.europa.eu | - ENISA European. Network and Inform. Assurance Agency |
| http://www.etsi.org/ | - ETSI European Telecommunications Standards Institute |
| http://www.caida.org | - CAIDA: The Center for Applied Internet Data Analysis |
| http://www.cert.org | - CERT - Coordination Center |
| http://www.sans.org | - SANS (SysAdmin, Audit, Network, Security) Institute |
| http://www.us-cert.gov | - US-CERT (Computer Emergency Readiness Team) |

**Διεθνή πρότυπα :**

**1) ISO (International Organization for Standardization – Ελβετία - (επί πληρωμή)**

ISO/IEC 27000 Information security management systems, Overview and vocabulary
ISO/IEC 27001 Information technology - Security Techniques – Information security management systems — Requirements.
ISO/IEC 27002 Code of practice for information security management
ISO/IEC 27003 Information security management system implementation guidance
ISO/IEC 27004 Information security management — Measurement
ISO/IEC 27005 Information security risk management

**2) NIST - National Institute of Standards and Technology - ΗΠΑ - (δωρεάν)**

NIST SP 800-12 An Introduction to Computer Security
NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
NIST SP 800-18 Guide for Developing Security Plans for Information Technology Systems
NIST SP 800-27 Engineering Principles for Information Technology Security
NIST SP 800-30 Risk Management Guide for Information Technology Systems

**Πιστοποιήσεις για επαγγελματίες στο χώρο της Ασφάλειας Πληροφοριών**

CISSP Certified Information Systems Security Professional (από τις γνωστότερες)

# Παράρτημα 2. Οδηγός Δημιουργίας Εικονικής Μηχανής

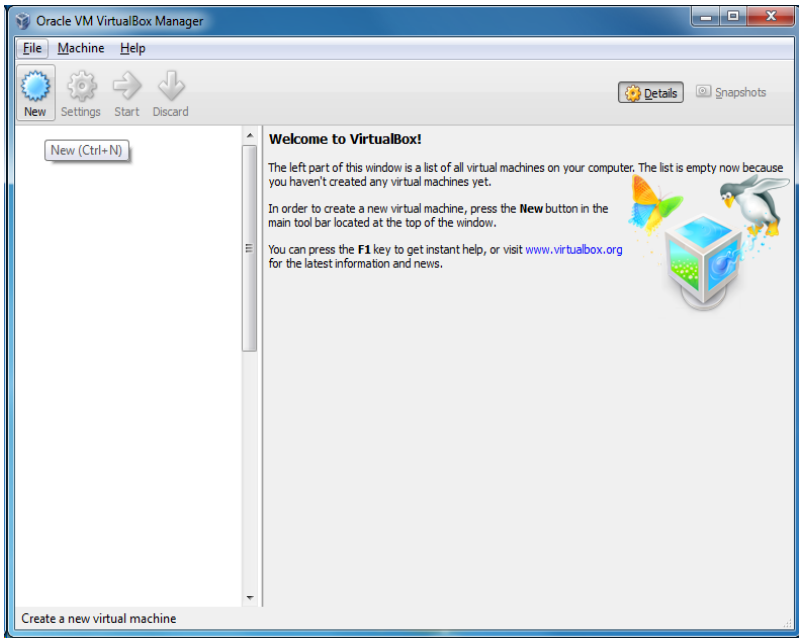
Το παράρτημα αυτό αναφέρεται στο κεφάλαιο 6 και είναι ενας οδηγός δημιουργίας Εικονικής Μηχανής και εκκίνησης εγκατάστασης ΛΣ Ubuntu Linux από το αρχείο *ubuntu-14.04.1-desktop-i386.iso*
(Οι **άδειες χρήσης** λειτουργικών συστημάτων και προγραμμάτων σε εικονικές μηχανές ακολουθούν τους νομικούς κανόνες που ισχύουν και στους φυσικούς υπολογιστές.)

**Έναρξη οδηγού δημιουργίας εικονικής μηχανής**

Επιλέγοντας ***New*** από τη γραμμή εργαλείων θα ξεκινήσει ο οδηγός για τη δημιουργία εικονικής μηχανής.

Ο οδηγός θα ζητήσει βήμα-βήμα όλα όσα χρειάζονται.

Στο τέλος κάθε βήματος πρέπει να πατηθεί το κουμπί **Next.**




Παράρτημα 2 - Εικόνα 1 - Έναρξη οδηγού δημιουργίας VM

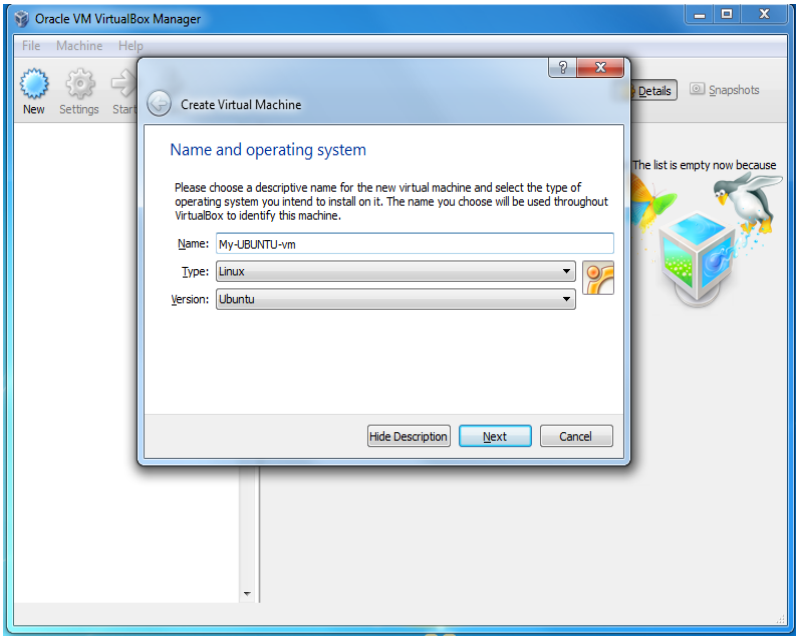
**Όνομα και είδος ΛΣ**

Στο πρώτο βήμα της διαδικασίας ζητούνται:

α) το όνομα (Name) της εικονικής μηχανής

β) το είδος (Type) του ΛΣ που θα εγκατασταθεί

γ) την έκδοση (Version) ΛΣ (πχ Ubuntu)



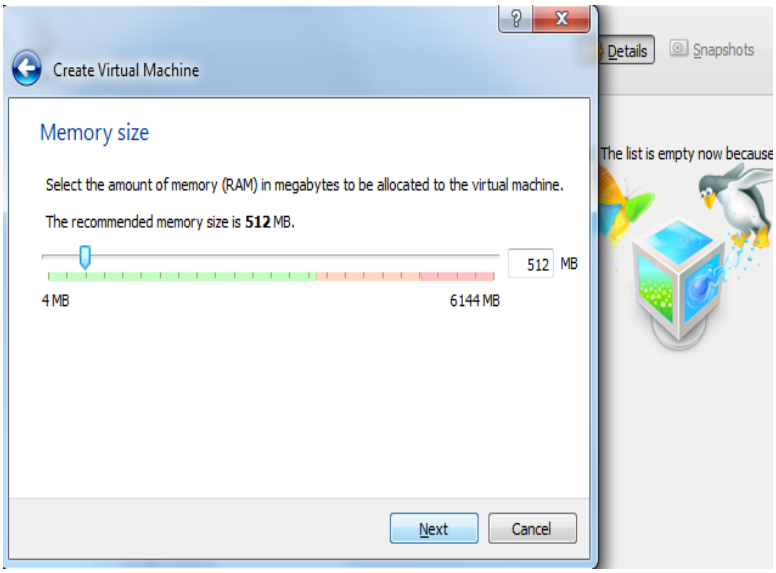

Παράρτημα 2 – Εικόνα 2 – Εισαγωγή ονόματος, ΛΣ, έκδοσης ΛΣ

**Επιλογή μεγέθους μνήμης RAM:**

Δήλωση μεγέθους της φυσικής μνήμης RAM που θα είναι διαθέσιμη στην Εικονική Μηχανή

Η τιμή αυτή μπορεί να αλλάξει αργότερα από τις ρυθμίσεις (settings).

Ο Επόπτης προτείνει τουλάχιστο 512 Mb (συνολικά υπάρχουν 6144 Mb μνήμης RAM)




Παράρτημα 2 – Εικόνα 3 – Επιλογή μεγέθους RAM

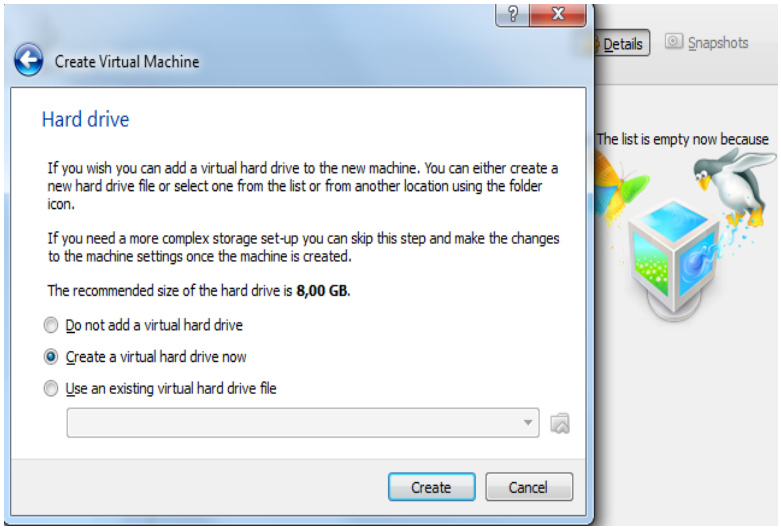
**Επιλογή ή δημιουργία εικονικού σκληρού δίσκου**

Τώρα μπορεί να επιλεχθεί:

α) να μη δημιουργηθεί δίσκος (θα προστεθεί χειροκίνητα αργότερα)

β) Άμεση δημιουργία δίσκου

γ) χρήση υπάρχοντα δίσκου

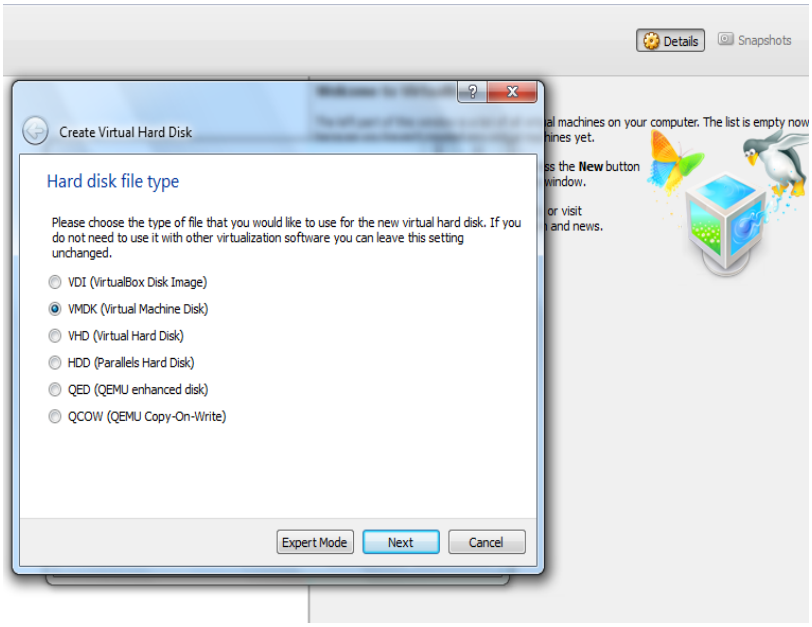



Παράρτημα 2 – Εικόνα 4 – Επιλογή σκληρού δίσκου

**Επιλογή είδους εικονικού δίσκου**

Κάθε είδος δίσκου προέρχεται από το αντίστοιχο πρόγραμμα. Ο δίσκος VDI είναι του VirtualBox, ενώ ο VMDK είναι του VMware Player.

Η επιλογή VMDK είναι θα διευκολύνει την χρησιμοποίησή του αργότερα και από το VMware Player.



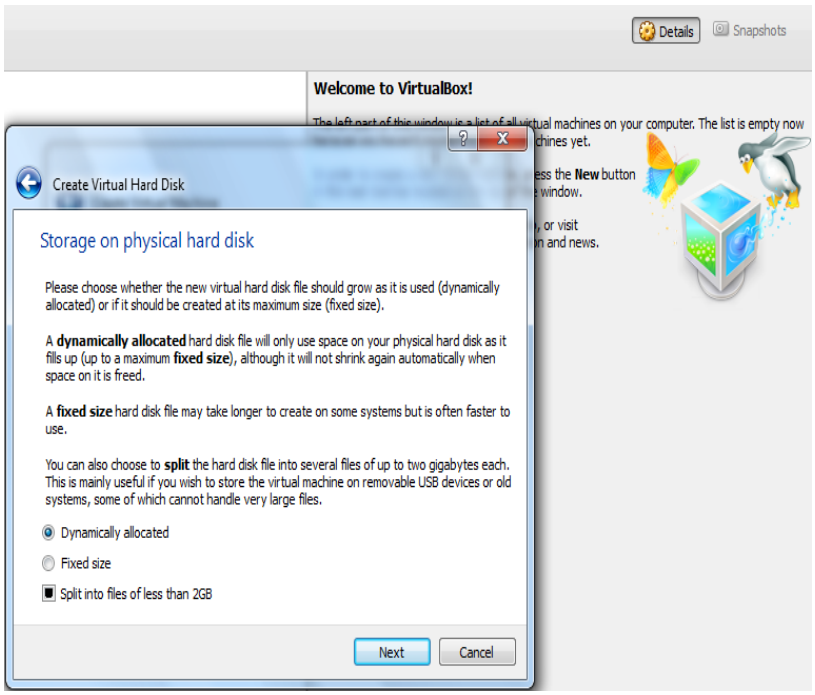

Παράρτημα 2 – Εικόνα 5 – Επιλογή τύπου εικονικού δίσκου

**Επιλογή τρόπου δέσμευσης χώρου από το φυσικό δίσκο.**

Δυναμική δέσμευση (***Dynamically allocated***). Για να μη δεσμευτεί άμεσα ο χώρος από τον εικονικό δίσκο αλλά να αυξάνεται όποτε χρειάζεται χώρο.

Σταθερό (***Fixed***), καταλαμβάνει άμεσα τα Gb που θα του δοθούν.

Η επιλογή ***Split into…*** θα δημιουργήσει αρχεία μεγέθους μέχρι 2 Gb για ευκολία μεταφοράς και δυνατότητα αποθήκευσης σε όλα τα συστήματα αρχείων (πχ το FAT32 έχει όριο τα 4Gb)

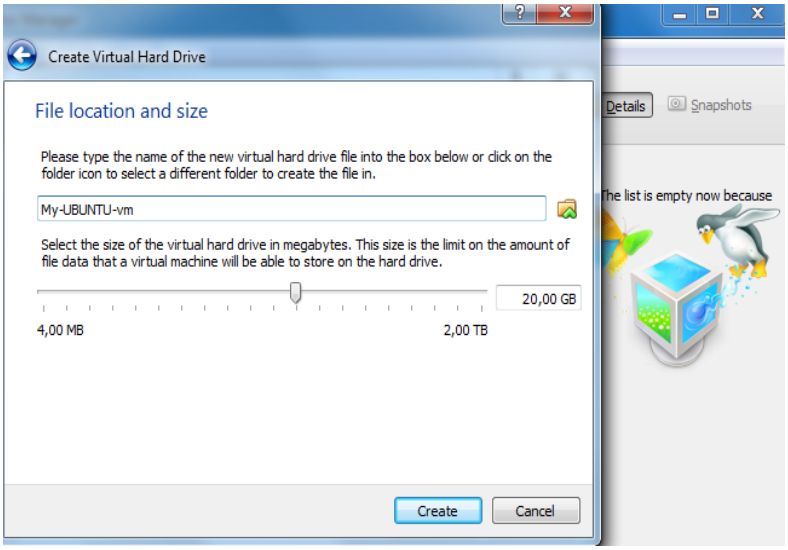



Παράρτημα 2 – Εικόνα 6 – Επιλογή τρόπου δέσμευσης

**Τελικό βήμα δημιουργίας εικονικής μηχανής**

-Επιλογή ονόματος δίσκου και φακέλου αποθήκευσης εικονικού δίσκου και
- μεγέθους δίσκου,

Εδώ μπορεί να γραφεί το επιθυμητό όνομα και ο φάκελος στον οποίο θα αποθηκευτεί (κίτρινο εικονίδιο με πράσινο ∧).

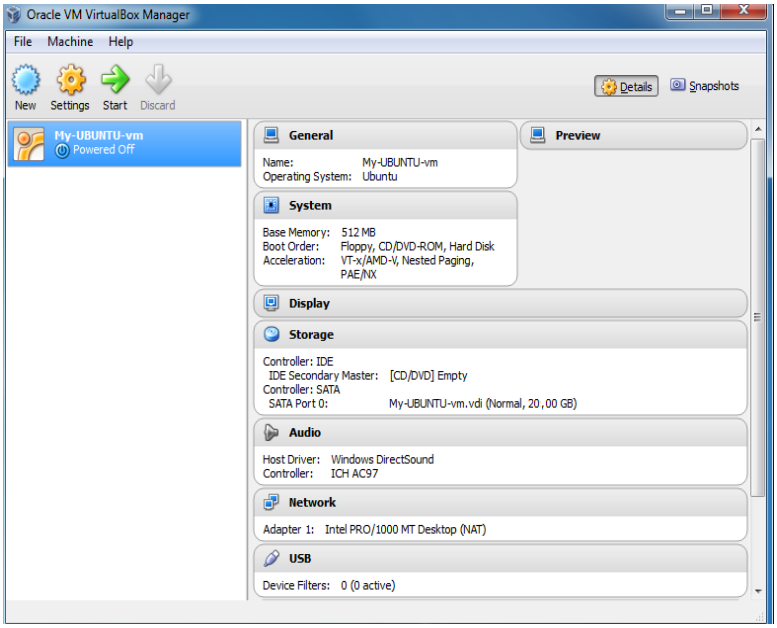



Παράρτημα 2 – Εικόνα 7 – Δημ. και φάκελος αποθήκευσης VM

Το μέγεθος του εικονικού δίσκου για σύγχρονες και πλήρεις εκδόσεις Linux θα πρέπει να είναι τουλάχιστον 10 Gb.

Πατώντας το *Create* θα δημιουργηθεί ο δίσκος και θα τερματίσει ο οδηγός δημιουργίας της μηχανής.

Αυτή θα είναι η εικόνα του Επόπτη μετά τη δημιουργία της εικονικής μηχανής (χωρίς ΛΣ όμως ακόμα).




Παράρτημα 2 – Εικόνα 8 – Εικόνα Επόπτη με VM

**Επιλογή του αρχείου εικόνας δίσκου (.iso) από όπου θα εγκατασταθεί ΛΣ**

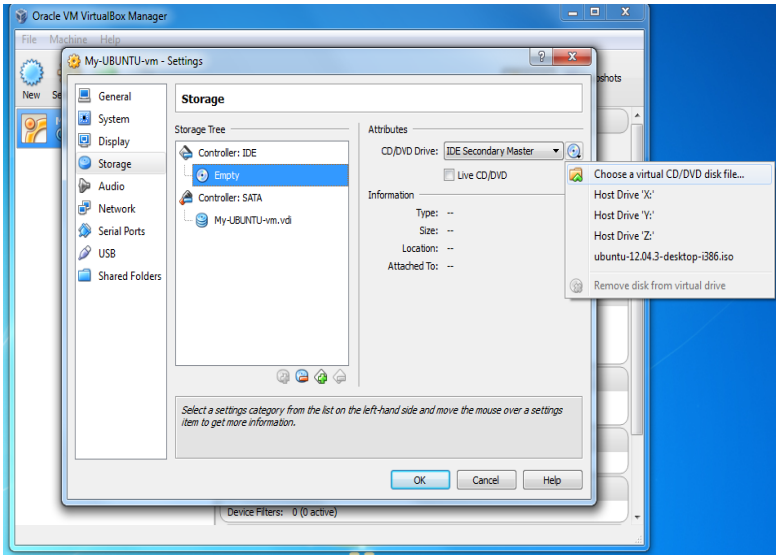
Θα επιλεχθεί το αρχείο *ubuntu-14.04.1-desktop-i386.iso* (ιστοσελίδα Ubuntu http://releases.ubuntu.com/14.04/ )

**Βήματα:**

Από τη γραμμή εργαλείων ***Settings / Storage*** και επιλογή:

1) του εικονιδίου cd κάτω από το *Controler IDE*

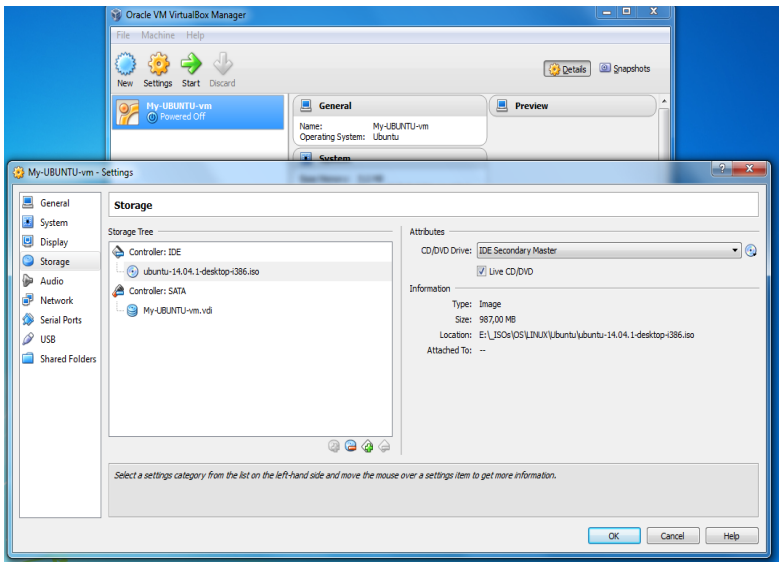
2) του εικονιδίου cd δεξιά από *IDE Secondary Master* για επιλογή του επιθυμητού αρχείου .iso




Παράρτημα 2 – Εικόνα 9 - Επιλογή εικόνας δίσκου .iso

Εάν έχει γίνει επιλογή του σωστού αρχείου, τότε δίπλα από το εικονίδιο *cd* που είναι κάτω από το *Controller IDE* θα εμφανιστεί το όνομα του .iso αρχείου *ubuntu-14.04.1-desktop-i386.iso*

**Μετά το πάτημα του κουμπί *OK* ο εικονικός υπολογιστής είναι έτοιμος για να εκκινήσει από το κουμπί *Start* και να εγκατασταθεί το ΛΣ** που υπάρχει στο αρχείο *ubuntu-14.04.1-desktop-i386.iso*

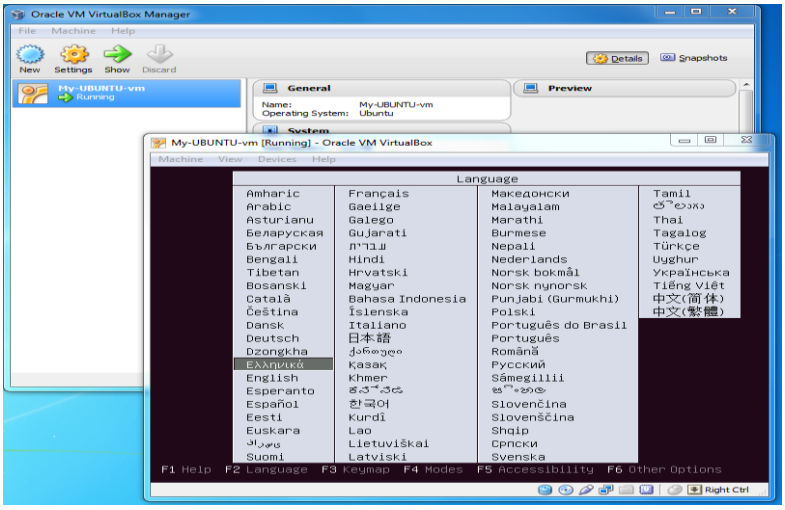



Παράρτημα 2 – Εικόνα 10 – Έλεγχος επιλεγμένου .iso

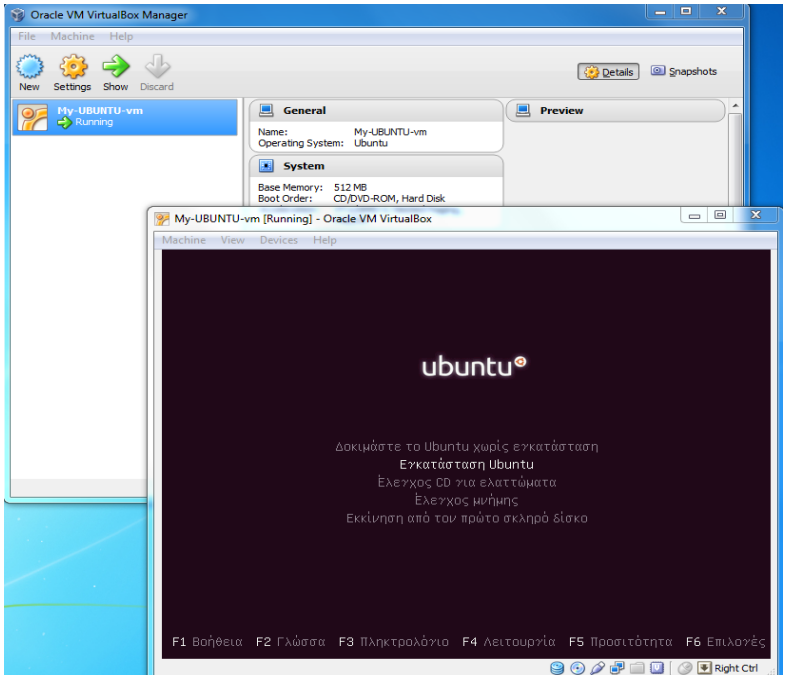
### Έναρξη εγκατάστασης ΛΣ στην εικονική μηχανή

Πατώντας το κουμπί ***Start*** της γραμμής εργαλείων θα κάνει εκκίνηση (boot) η εικονική μηχανή και θα κάνει αρχίσει η διαδικασία εγκατάστασης του Ubuntu Linux που συνδέθηκε με τον εικονικό οδηγό cd.

Από το σημείο αυτό και μετά, όλα τα βήματα ακολουθούν αυτά μιας τυπικής εγκατάστασης σε φυσικό υπολογιστή. Η μόνη διαφορά είναι πως εδώ όλα γίνονται μέσα σε έναν φάκελο και δεν κινδυνεύουν τα αρχεία του φυσικού υπολογιστή από λάθη, κατά την εγκατάσταση αλλά και αργότερα, μετά την εγκατάσταση ΛΣ.




Παράρτημα 2 – Εικόνα 11 – Εκκίνηση από το .iso




Παράρτημα 2 – Εικόνα 12 – Έναρξη εγκατάστασης Ubuntu

**ΤΕΛΟΣ ΟΔΗΓΟΥ δημιουργίας και εγκατάστασης ΛΣ Ubuntu σε Εικονική Μηχανή**

# Δικτυογραφία


**Κεφ.1-4**

1. *https://ellak.gr/* Ελληνική ιστοσελίδα για το Ελεύθερο Λογισμικό
2. *http://www.bandwidthco.com/os.html*. Ιστοσελίδα με πληροφορίες για θέματα διαχείρισης των λειτουργικών συστημάτων Windows και Linux.
3. *http://windows.microsoft.com/en-us/windows/windows-basics-all-topics*. Ιστότοπος της Microsoft με πληροφορίες για τα Windows και τους υπολογιστές.
4. *http://www.ubuntu.com/*. Ο ιστότοπος της διανομής Ubuntu του Linux
5. *http://www.dewassoc.com/kbase/hard_drives/hard_drive_glossary.htm*. Ιστοσελίδα με γλωσσάρι ορολογίας σκληρών δίσκων.
6. *http://www.adrc.com/ckr_main.html*. Ιστοσελίδα με πηγές πληροφόρησης για υπολογιστές
7. *http://docs.oracle.com/en/operating-systems/*
8. *http://www.pcsteps.gr/* Ιστότοπος με οδηγίες και λύσεις σε τεχνικά θέματα
9. *http://www.demsym.com/index.php/mathimata/a-gymnasiou/item/39-a-katigories-logismikou-kai-leitourgiko-systima* *Ιστότοπος με εκπαιδευτικό υλικό για Πληροφορική*

**Κεφ.5**

1. *https://en.wikipedia.org/wiki/CERT_Coordination_Center*
2. *https://cert.grnet.gr/*
3. *http://cert.sch.gr*
4. *http://ciso.washington.edu/information-security-and-privacy-risk-management/*
5. *http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf*
6. *http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf*
7. *http://firstmonday.org/ojs/index.php/fm/article/view/778/687*
8. *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*
9. *http://support.gpgtools.org/kb/how-to/add-more-email-addresses-user-ids-to-your-existing-key*
10. *http://windows.microsoft.com/el-gr/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7*
11. *http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&langENENENEN*
12. *http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html*
13. *http://www.coe.int/el/web/cybercrime/home*
14. *http://www.dpa.gr/pls/portal/url/ITEM/432C7C07FB600EEDE040A8C07D2451D3*
15. *http://www.dpa.gr/portal/page?_pageid=33,132277&_dad=portal&_schema=PORTAL*
16. *http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html*
17. *http://www.eicar.org/85-0-Download.html*
18. *http://www.sans.org/critical-security-controls/*

19. *http://www.sans.org/security-resources/policies/*
20. *http://www.sans.org/reading-room/whitepapers/sysadmin/backup-rotations-final-defense-305*
21. *http://datasitenw.com/common-backup-strategies*
22. *http://www.security.mtu.edu/policies-procedures/information-security-plan.pdf*
23. *http://www.symantec.com/connect/articles/introduction-trojans-and-backdoors*
24. *http://www.techopedia.com/definition/24840/information-systems-security-infosec*
25. *http://www.trendmicro.com/vinfo/us/security/definition/Ransomware*
26. *https://el.wikipedia.org/wiki/Ασφάλεια_πληροφοριακών_συστημάτων*
27. *https://en.wikipedia.org/wiki/Information_security*
28. *https://pki.grnet.gr/*
29. *https://pki.grnet.gr/help*
30. *https://support.microsoft.com/el-gr/kb/136621*
31. *https://support.microsoft.com/el-gr/kb/841290*
32. *https://support.office.com/en-IE/Article/get-or-create-your-own-digital-signature-e3d9d813-3305-4164-a820-2e063d86e512*
33. *https://www.enisa.europa.eu*
34. *https://www.grc.com/misc/truecrypt/truecrypt.htm*
35. *http://www.syros.aegean.gr/users/lekkas/pubs/t/dlek_thesis_final.htm*
36. *https://www.issa.org*
37. *https://www.comodo.com/home/email-security/free-email-certificate.php*
38. *https://openvpn.net/index.php/open-source/downloads.html*

**Κεφ. 6**

1. *https://www.virtualbox.org/*
2. *https://www.virtualbox.org/manual/ch01.html#virtintro*
3. *http://www.vmware.com/virtualization/how-it-works.html*

# Βιβλιογραφία

**Κεφ.1-4**


1. Welsh M, Dalheimer M.K, Kaufman L, "Running Linux", O'Reilly, 1999
2. Αράπογλου Α., Μαβόγλου Χ., Οικονομάκος Η., Φύτρος Κ, «Πληροφορική Α',Β',Γ' Γυμνασίου», Παιδαγωγικό Ινστιτούτο, 2006
3. Γεωργίου Θ., Κάππος Ι., Λαδιάς Α., Μικρόπουλος Α., Τζιμογιάννης Θ., Χαλκιά Κ., «Πολυμέσα-Δίκτυα», Παιδαγωγικό Ινστιτούτο,1999
4. Γιακουμάκης Ε., Γκυρτής Κ., Μπελεσιώτης Β.Σ, Ξυνός Π., «Εφαρμογές Πληροφορικής-Υπολογιστών Α΄, Β΄, Γ΄ Ενιαίου Λυκείου», ΟΕΔΒ, 2000
5. Γώγουλος Π., Εξαρχάκος Π., Ζήσου Α., Κάβουρας Ι., Λιβαδάς Κ. «Λειτουργικά Συστήματα», ΟΕΔΒ, Παιδαγωγικό Ινστιτούτο, 2002
6. Κάβουρα Ι., Συστήματα Υπολογιστών ΙΙ Λειτουργικά Συστήματα, 3η έκδοση, Εκδόσεις Κλειδάριθμος, 1995
7. Tanenbaum, A.S, «Σύγχρονα Λειτουργικά Συστήματα», τόμος Α, εκδόσεις Παπασωτηρίου, 1993
8. Meyers M., «Εισαγωγή στο PC Hardware και στην αντιμετώπιση προβλημάτων», Εκδόσεις Γκιούρδας, 2005
9. Παπακωνσταντίνου Γ., Τσανάκας Π, Κοζύρης Ν., Μανουσοπούλου Α., Ματζάκος Π., «Τεχνολογία Υπολογιστικών Συστημάτων και Λειτουργικά Συστήματα», Βιβλίο Μαθητή, ΙΤΥΕ «Διόφαντος»,1999
10. Παπακωνσταντίνου Γ.Κ, Μπιλάλης Ν.Α, Τσανάκας Π.Δ, «Λειτουργικά Συστήματα, Μέρος Ι: Αρχές Λειτουργίας», Εκδόσεις Συμμετρία, Αθήνα 1986


**Κεφ.5-6**


11. Umesh Hodeghatta and Umesha Nayak, "The InfoSec Handbook", Apress ISBN13: 978-1-4302-6382-1, 2014
12. Stewart J. M., Tittel Ed, Chapple M, "CISSP Certified Information Systems Security Professional Study Guide 4th Edition" , Wiley Publishing ISBN: 978-0-470-27688-4,2008
13. Κάτσικα Σ. Γκρίτζαλη Δ., «*Ασφάλεια Πληροφοριακών Συστημάτων*», Εκδόσεις Νέων Τεχνολογιών, 2004. ISBN13: 978-960-8105-57-7