



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Ασφάλεια Πληροφοριακών Συστημάτων στην Τριτοβάθμια Εκπαίδευση

ΚΟΥΚΟΠΟΥΛΟΣ ΝΙΚΟΛΑΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Δαδαλιάρης Αντώνιος

Επίκουρος Καθηγητής

Λαμία έτος 2024



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Ασφάλεια Πληροφοριακών Συστημάτων στην Τριτοβάθμια Εκπαίδευση

ΚΟΥΚΟΠΟΥΛΟΣ ΝΙΚΟΛΑΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Δαδαλιάρης Αντώνιος

Επίκουρος Καθηγητής

Λαμία έτος 2024



UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

Information Systems Security in Higher Education

KOUKOPOULOS NIKOLAOS

FINAL THESIS

ADVISOR

Antonios Dadaliaris

Assistant Professor

Lamia year 2024

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις ⁽¹⁾, που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.
2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.
3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια
4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία:/...../20.....

Ο - Η Δηλ.

ΕΥΧΑΡΙΣΤΙΕΣ

*Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου **Δαδαλιάρη Αντώνιο, Επίκουρο Καθηγητή**, για την καθοδήγηση που μου προσέφερε και το χρόνο που διέθεσε δίνοντάς μου χρήσιμες συμβουλές και οδηγίες για την ολοκλήρωση της πτυχιακής μου εργασίας.*

Στο ίδιο πλαίσιο ευγνωμοσύνης, θα ήθελα να ευχαριστήσω όλους τους καθηγητές του τμήματος Πληροφορικής και Τηλεπικοινωνιών - ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΘΕΣΣΑΛΙΑΣ για τη συμβολή τους στην επιστημονική και τεχνολογική μου συγκρότηση στα χρόνια της φοίτησής μου στο Τμήμα.

Οφείλω επίσης ένα μεγάλο ευχαριστώ σε όλους εκείνους που συνέβαλαν είτε πρακτικά είτε ψυχικά (βοήθεια και παραινέσεις) στην ολοκλήρωση της εργασίας μου.

Τέλος, ένα μεγάλο ευχαριστώ στους γονείς μου για την οικονομική τους υποστήριξη, καθώς και τους συγγενείς και τους φίλους για την ηθική υποστήριξη σε όλο το διάστημα των σπουδών μου.

ΠΕΡΙΛΗΨΗ

Η σημερινή εποχή χαρακτηρίζεται από μια ιδιαίτερη μεγάλη ανάπτυξη και γενικευμένη χρήση της τεχνολογίας της πληροφορικής και των επικοινωνιών. Οι υπολογιστές χρησιμοποιούνται σήμερα σε όλες τις ανθρώπινες δραστηριότητες και κάθε είδους εργασίες, εμπορικές, επιστημονικές κλπ. Παράλληλα όμως αυξάνονται οι κίνδυνοι και τα κρούσματα από ηθελημένες ή τυχαίες καταστροφές, αλλοιώσεις ή μη εξουσιοδοτημένη χρήση των δεδομένων και γενικότερα των υπολογιστικών πόρων. Οι συνέπειες από πιθανές καταστροφές, αλλοιώσεις, ή κακή χρήση δεδομένων μπορεί να σημαίνουν όχι μόνο υλικές ζημιές και κόστη αλλά και κινδύνους για την προστασία των ατομικών δικαιωμάτων των πολιτών. Πιο συγκεκριμένα, η εργασία μας θα ασχοληθεί με την ασφάλεια των πληροφοριακών συστημάτων. Στο 1ο κεφάλαιο θα αναφερθούμε στη τριτοβάθμια εκπαίδευση σε ότι αφορά την ασφάλεια των πληροφοριακών συστημάτων και θα αναφερθούμε στα πανεπιστημιακά ιδρύματα που έχουμε συλλέξει και την διαδρομή των πανεπιστημίων από την οπτική γωνία της πληροφορικής και ασφάλειας των πληροφοριακών συστημάτων. Στο 2ο κεφάλαιο θα δώσουμε αναλυτικά τις εννοιολογικές εννοείς ότι αφορά την ασφάλεια των πληροφοριακών. Στο κεφάλαιο 3 θα δώσουμε αναλυτική παρουσίαση των πανεπιστημιακών ιδρυμάτων στο τι περιλαμβάνεται στα μαθήματα σπουδών στον τομέα της πληροφορικής και συγκεκριμένα στον τομέα της ασφάλειας των πληροφοριακών συστημάτων. Στο κεφάλαιο 4, θα παρουσιάσουμε αναλυτικά στατιστικά πάνω στην έρευνα που έχουμε διεκπεραιώσει όσον αφορά το τι αναφέρεται στο μάθημα της ασφάλειας των πληροφοριακών συστημάτων σε πολλούς τομείς που θα εξετάσουμε. Στο τελευταίο 5 κεφάλαιο θα καταγράψουμε τα συμπεράσματα που διακρίνουμε στο προηγούμενο κεφαλαίου για την έρευνα που κάναμε.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ : ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑΛΕΞΕΙΣ
ΚΛΕΙΔΙΑ: ασφάλεια, πληροφοριακά συστήματα, κυβερνοασφάλεια, δεδομένα
,λογισμικό, πληροφορία

ABSTRACT

Today's era is characterized by a particular large use and general use of information and communication technology. Computers today series in all human activities and all kinds of work, commercial, scientific, etc. At the same time, the risks and cases of intentional or accidental disasters, alterations or unauthorized use of data and computing resources in general are increasing. The consequences of possible destruction, alteration, misuse of data can mean not only material damages and costs but also risks for the protection of the individual rights of citizens. More specifically, our work will deal with the security of information systems. In the 1st chapter we will refer to higher education in terms of information systems security and we will refer to the universities we have collected and the path of the universities from the perspective of IT and information systems security. In chapter 3 we will give a detailed presentation of the university institutions in what is included in the courses of studies in the field of information technology and specifically in the field of security of information systems. a lesson in the security of information systems in many areas that we will examine. In the last 5 chapters, we will record the conclusions we distinguish in the previous chapter for the research we did.

SUBJECT AREA: SECURIY OF INFORMATION SYSTEMS

KEY WORDS: security, information system, cyber security, data, software, information

ΚΑΤΑΛΟΓΟΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΞΩΦΥΛΛΟ.....	1
ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ.....	7
ΕΥΧΑΡΙΣΤΗΣΙΕΣ.....	9
ΠΕΡΙΛΗΨΗ.....	10
ABSTRACT	11
ΠΡΟΛΟΓΟΣ	14
ΚΕΦΑΛΑΙΟ 1 ΕΙΣΑΓΩΓΗ.....	16
ΕΝΟΤΗΤΑ 1.1.....	17
ΕΝΟΤΗΤΑ 1.2.....	18
ΚΕΦΑΛΑΙΟ 2 ΒΑΣΙΚΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ.....	19
2. ΕΝΝΟΙΑ ΣΥΣΤΗΜΑΤΟΣ ΣΤΗΝ ΠΛΗΡΟΦΟΡΙΚΗ.....	19
2.1 ΙΔΙΟΤΗΤΕΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ.....	20
2.2 ΕΝΝΟΙΑ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ.....	20
2.3 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΤΟΥ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ.....	24
2.4 ΘΕΜΕΛΙΩΔΗΣ ΕΝΝΟΙΕΣ ΤΟΥ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ	26
2.5 ΔΕΥΤΕΡΕΥΟΥΣΕΣ ΕΝΝΟΙΕΣ ΠΣ.....	28
2.6 ΠΑΡΑΒΙΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ.....	29
2.7 ΕΥΠΑΘΕΙΕΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ.....	30
2.8 ΑΠΕΙΛΕΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ.....	31
2.19 ΚΑΤΗΓΟΡΙΕΣ ΑΠΕΙΛΩΝ	32
2.10 ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ.....	33
2.11 ΤΟΠΟΘΕΤΗΣΗ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ ΣΕ ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ.....	35
ΚΕΦΑΛΑΙΟ 3. ΑΝΑΛΥΤΙΚΗ ΠΑΡΟΥΣΙΑΚΗ ΤΜΗΜΑΤΩΝ.....	39
1. ΣΧΟΛΗ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ.....	39
2. ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ.....	42
3. ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ (Ο.Π.Α.).....	43
4. ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ(Α.Π.Θ.).....	46
5. ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ(Ι.Π.).....	47
6. ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ(ΠΑ.ΠΕΙ.).....	52
7. ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ	54
8. ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ(Ε.Κ.Π.Α.).....	55
9. ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ(ΠΑ.ΠΕΛ.).....	56
10. ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ (Π.Θ.).....	57
11. ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΒΙΟΙΑΤΡΙΚΗ.....	59

12. ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ(Π.ΙΩΝ.).....	60
13. ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ(Π.ΠΑΤΡΩΝ).....	62
14. ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ	67
ΚΕΦΑΛΑΙΟ 4 ΠΑΡΟΥΣΙΑΣΗ ΣΤΑΤΙΣΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ ΕΡΕΥΝΑΣ.....	71
ΚΕΦΑΛΑΙΟ 5 ΑΠΟΤΕΛΕΣΜΑΤΑ-ΣΥΜΠΕΡΑΣΜΕΡΑΣΜΑΤΑ.....	76
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	78

ΠΡΟΛΟΓΟΣ

Στα πλαίσια του Προγράμματος Προπτυχιακών Σπουδών με κατεύθυνση την πληροφορική ,εκπονήθηκε η παρούσα πτυχιακή εργασία του «Τμήματος Πληροφορικής και Τηλεπικοινωνιών» του Πανεπιστημίου Θεσσαλίας. Στην εργασία αυτή εξετάζεται η ασφάλεια των πληροφοριακών συστημάτων στην Τριτοβάθμια Εκπαίδευση.

Η πτυχιακή εργασία ξεκίνησε τον Μάρτιο του 2024 και ολοκληρώθηκε μέσα σε σύντομο χρονικό διάστημα με την υποβολή της συγκεκριμένης εργασίας. Η έρευνα για το θέμα πραγματοποιήθηκε καθ' όλη τη διάρκεια της εκπόνησης της πτυχιακής.

Αρχικά, στην καθημερινότητα μας συναντάμε το φαινόμενο της κλοπής δεδομένων το οποίο συμβαίνει σε μεγάλο ποσοστό στα πληροφοριακά συστήματα για οποιαδήποτε χρήση γίνεται είτε είναι για προσωπικό επίπεδο είτε για Πανεπιστημιακό επίπεδο.

Επιπλέον, εάν αυτό το πρόβλημα συνεχίσει να εμφανίζεται τακτικά, θα μας αναγκάσει να ενισχύσουμε τα μέτρα ασφαλείας των πληροφοριακών μας συστημάτων, με στόχο να προλάβουμε περαιτέρω επαναλήψεις του.

Τέλος, θα μελετήσουμε αναλυτικά ένα μέρος από τα Πανεπιστημιακά Ιδρύματα, το τι κάνουν πάνω σε αυτόν τομέα του μαθήματος ,δηλαδή στην ασφάλεια των πληροφοριακών συστημάτων, και θα τα συγκρίνουμε μεταξύ τους.

Έτσι λοιπόν, ο σκοπός της παρούσας εργασία είναι να δώσουμε τις μεν εννοιείς για την ασφάλειά αλλά και τις δε αναλύσεις και συγκρίσεις των πανεπιστημίων όσον αφορά για την ασφάλεια των πληροφοριακών συστημάτων.

ΚΕΦΑΛΑΙΟ 1: Εισαγωγή

ΤΡΙΤΟΒΑΘΜΙΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

1.1 ΕΙΣΑΓΩΓΗ

Η ασφάλεια πληροφοριών αποτελεί κρίσιμο ζήτημα στα νεότερα πληροφοριακά συστήματα. Η ενσωμάτωση προηγμένων τεχνικών και τεχνολογιών, όπως σύγχρονες βάσεις δεδομένων και δικτυακές υποδομές, παρέχει μεν μεγάλα οφέλη και δυνατότητες, αυξάνει όμως ταυτόχρονα και τις προκλήσεις που συνδέονται με την προστασία και τη διαθεσιμότητα των πληροφοριών. Στο πλαίσιο ενός πληροφοριακού συστήματος, όπως εκείνο ενός νοσοκομείου, είναι αναγκαίο να διασφαλιστεί ότι οι προσωπικές και ευαίσθητες πληροφορίες του ασθενούς, που καταχωρίζονται κατά την εισαγωγή του ή δημιουργούνται κατά τη διάρκεια της θεραπείας, συλλέγονται, αποθηκεύονται και επεξεργάζονται με τρόπο που εξασφαλίζει την ακεραιότητα, την ασφάλεια και την προσβασιμότητα από εξουσιοδοτημένους μόνο χρήστες, σύμφωνα με τη νομοθεσία. [3]

Η ικανοποίηση των απαιτήσεων για την ασφάλεια των πληροφοριακών συστημάτων είναι συνεπώς μια από τις βασικότερες προϋποθέσεις για την εισαγωγή και αξιοποίηση της τεχνολογίας της πληροφορικής. [3]

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας (ποιότητα, απόδοση κλπ.) για την εξασφάλιση της εύρυθμης λειτουργίας ενός οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σήμερα όπου πολύ συχνά το σύνολο παρεχόμενων υπηρεσιών ενός οργανισμού στηρίζεται στην πληροφορική (πχ πάνω από το 80% των υπηρεσιών μιας τράπεζας). [3]

Τέλος, για να μπορούμε να λύσουμε αυτό το πρόβλημα πρέπει να παρέχετε ασφάλεια σε κάθε πληροφοριακό σύστημα. Έτσι θα μελετήσουμε την ασφάλεια των πληροφοριακών συστημάτων και με ποιον τρόπο μεταδίδεται σε κάθε πανεπιστήμιο ξεχωριστά. [3]

ΣΚΟΠΟΣ ΕΡΕΥΝΑΣ

Ο σκοπός της ερευνάς είναι η αναγνώριση της εννοίας της ασφάλειας των πληροφοριακών συστημάτων και η ανάλυση των μαθημάτων σε πανεπιστημιακό επίπεδο. Όπου θα αναλύσουμε ξεχωριστά το καθένα, το πως μεταδίδεται ως μάθημα η ασφάλεια του ΠΣ(πληροφοριακού συστήματος) σε πανεπιστήμια που έχουμε συλλέξει. Άλλος ένας λόγος, που διεξάγουμε αυτή τη ερευνά είναι για να διαπιστώσουμε τι διαφορές υπάρχουν μεταξύ των πανεπιστημίων κατά την διεξαγωγή των μαθημάτων τους, τι χρησιμοποιούν για την διεξαγωγή (δηλαδή,

συγγράμματα, βιβλία, διαλέξεις),το περιεχόμενο του μαθήματος και άλλες παραμέτρους που θα αναφερθούν στο 4ο κεφάλαιο .

ΕΝΟΤΗΤΑ 1.1 : ΑΝΑΦΟΡΑ ΣΤΗΝ ΤΡΙΤΟΒΑΘΜΙΑ ΕΚΠΑΙΔΕΥΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΟΥ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Στην εργασία αυτή διερευνάμε την παρουσία του μαθήματος «Ασφάλεια Πληροφοριακών Συστημάτων» στην τριτοβάθμια εκπαίδευση σε προπτυχιακό επίπεδο στον τομέα της Πληροφορικής με κύριο σκοπό την ανάδειξη της κατάστασης που αναγράφεται για το μάθημα αυτό και το υλικό που διεξάγεται για την ασφάλεια των ΠΣ .Επιπλέον ο στόχος της εργασίας μας είναι η διερεύνηση των εκπαιδευτικών τάσεων ανάλογα με το είδος του εκπαιδευτικού ιδρύματος και το επίπεδο σπουδών στο οποίο διεξάγεται το μάθημα της ασφάλειας των ΠΣ .Μέσα από τις οποίες θα προκύψουν πολλές διαφορές ανάλογα από το εκπαιδευτικό ίδρυμα που θα εξετάσουμε και μας τεθούν διάφοροι προβληματισμοί σχετικά με το πως θα διεξάγεται το μάθημα της ασφάλειας στον τομέα της πληροφορικής και αν μέσα από αυτές τις κατευθύνσεις που δίνει η τριτοβάθμια εκπαίδευση να δούμε αν τα εφόδια που δίνονται στο μάθημα ,οι υποψήφιοι μπορούν να τα χρησιμοποιήσουν και να τα εφαρμόσουν με σωστό τρόπο στα ΠΣ όπου εργάζονται. Διαπιστώθηκε ότι σε μεγάλο βαθμό το υλικό του μαθήματος που διδάσκετε εστιάζετε σε εισαγωγικές έννοιες καθώς και το πρακτικό κομμάτι σε όλα τα πανεπιστήμια γίνεται σε πολύ μικρή εφαρμογή και έτσι δεν υπάρχει δυνατότητα ουσιαστικής εφαρμογής στην ασφάλεια των μοντέρνων ΠΣ .Η τεχνολογία που υπάρχει εξελίσσεται συνεχώς και η ασφάλεια των πληροφοριακών συστημάτων πρέπει να γίνεται πιο εντατικά στα νέα ΠΣ και πρέπει να δοθούν τα καταλληλά προνομία από την εκπαίδευσή για επιτευχθούν οι στόχοι της επαρκούς ασφάλειας σε κάθε σύστημα, είτε σε πανεπιστημιακό επίπεδο είτε ακόμη και σε εταιρικό επίπεδο . Με την ασφάλεια που πρέπει να παρέχουμε στο σύστημα ,θα έχουμε ασφαλή όλα τα στοιχεία αλλά και δεδομένα που διακατέχει το ΠΣ .

ΕΝΟΤΗΤΑ1.2: ΔΙΑΔΡΟΜΗ ΤΩΝ ΠΑΝΕΠΙΣΤΗΜΙΩΝ ΑΠΟ ΤΗΝ ΠΛΗΡΟΦΟΡΙΚΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΣ

Η πληροφορική όπως γνωρίζουμε είναι μια επιστήμη με την οποία γίνεται συνδυασμός πολλών ορισμών και διαδικασιών. Μια από τις βασικές διαδικασίες που αναγνωρίζουμε στον τομέα της πληροφορικής είναι η ασφάλεια των πληροφοριακών συστημάτων . Την συναντάμε ως μάθημα είτε πρακτικό είτε μόνο θεωρητικό. Αρχικά, μπορούμε να πούμε ότι όλα έχουν ως αρχή ότι έχουμε μεγάλο ποσοστό πληροφοριών αλλά και δεδομένων και πρέπει με κάποιο τρόπο να τα μεταδώσουμε μέσω ενός ΠΣ σε πανεπιστημιακό επίπεδο .Δηλαδή, τα πανεπιστήμια εκφράζουν της βασικές εννοιές που έχει ένα ΠΣ για την κατανόηση της διαδικασίας της ασφάλειας. Στην συνέχεια, η πληροφορική μας δίνει την δυνατότητα να εργαστούμε σε ένα λογισμικό όπου υπάρχει στα πανεπιστήμια για την πρακτική ειδίκευση των υποψήφιων που καταρτίζονται σε αυτά. Μέσω της πληροφορικής και τον λογισμικών που διαθέτουμε έχουμε την δυνατότητα να μεταφέρουμε δεδομένα αλλά και πληροφορίες όπου κατά την μετάδοση τους μπορεί σε μεγάλο ποσοστό να προκύψει είτε υποκλοπή είτε κάτι διαφορετικό που μπορεί να εκθέσει τις προσωπικές πληροφορίες σε κίνδυνο, ανάλογα τον τομέα είτε πανεπιστημιακό, είτε εταιρικό. Δεν δίνεται τόσο έμφαση έτσι ώστε να οι υποψήφιοι να κατανοήσουν τι κίνδυνος υπάρχει και πως να εγκαταστήσουν την ασφάλεια αλλά δίνονται οι κατευθυντήριες γραμμές και βασικές γνώσεις με τους κατάλληλους ορισμούς.

Τέλος, στην παρούσα εργασία θα ασχοληθούμε με διαφορά πανεπιστημιακά ιδρύματα που συλλέξαμε για το πως διεξάγετε το μάθημα της ασφάλειας των ΠΣ και αν υπάρχει πρακτικό μέρος σε αυτό το κομμάτι ,τι αναφέρετε σε αυτό , στο θεωρητικό μέρος και πόση βαρύτητα δίνεται σε αυτό το μάθημα. [1]

ΚΕΦΑΛΑΙΟ 2 :Βιβλιογραφική Επισκόπηση

ΒΑΣΙΚΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

2. ΕΝΝΟΙΑ ΣΥΣΤΗΜΑΤΟΣ ΣΤΗΝ ΠΛΗΡΟΦΟΡΙΚΗ

Η έννοια του "συστήματος" παρουσιάζεται με πολλαπλές ερμηνείες στην καθημερινή χρήση. Στο πλαίσιο της συγκεκριμένης ανάλυσης, ο όρος "σύστημα" αναφέρεται σε ένα συνδυασμό συστατικών μερών που συνδέονται λειτουργικά μέσα σε μία οργανωμένη δομή, η οποία προκύπτει σε μία σειρά από δραστηριότητες με στόχο την επίτευξη μιας προκαθορισμένης αποστολής.

Ας εστιάσουμε στα κύρια στοιχεία που χαρακτηρίζουν κάθε σύστημα:

1. Ένα σύστημα μπορεί να αποτελείται από μια ενιαία δομή ή να περιλαμβάνει πολλαπλά στοιχεία, όπως υλικά συστατικά, ανθρώπινες δυνάμεις, οργανωτικές διαδικασίες ή πληροφορίες. Εάν ένα από τα στοιχεία αυτά εξυπηρετεί ανεξάρτητα ως σύστημα, τότε αυτό κατατάσσεται ως υποσύστημα.

2. Αν και τα συστατικά ενός συστήματος μπορεί να διαφέρουν μορφολογικά, υπάρχει σημαντική αλληλεπίδραση και συνεργασία μεταξύ τους. Αυτή η σύνδεση καθιστά την αξία του συστήματος αντιληπτή μόνο ως ενιαίο σύνολο, και όχι μέσω της ανάλυσης των μεμονωμένων μερών του.

3. Αυτή η αλληλεπίδραση όχι μόνο ορίζει αλλά και διευκολύνει τη λειτουργία του συστήματος, στοχεύοντας στην επίτευξη ενός συγκεκριμένου σκοπού με αποτελεσματικότητα. Έτσι, η συνολική αξία του συστήματος υπερβαίνει την αξία των επιμέρους στοιχείων του, καθώς επιτυγχάνεται ένα συνεργικό αποτέλεσμα. [3]

2.1 ΠΥΡΗΝΑΣ ΕΝΟΣ ΣΥΣΤΗΜΑΤΟΣ

Από τον παραπάνω ορισμό του "συστήματος", αναδεικνύονται κάποια βασικά ιδιότητες που απαιτούν ειδική αναφορά για την καλύτερη κατανόηση της λειτουργίας του. Αυτά περιλαμβάνουν:

1.Εισροές - Επεξεργασία - Εκροές: Αυτή η διαδικασία αποτελεί τον κύκλο λειτουργίας του συστήματος, όπου οι εισροές μετατρέπονται μέσω της επεξεργασίας σε εκροές, υπηρετώντας τον κύριο σκοπό του συστήματος και παρέχοντας την απαραίτητη κινητροδότηση για την ενεργοποίησή του.

2.Περιβάλλον του Συστήματος: Κάθε σύστημα λειτουργεί εντός ενός περιβάλλοντος που επηρεάζει τη λειτουργία του, ενώ ταυτόχρονα μπορεί να δέχεται επιδράσεις από αυτό σε διάφορους βαθμούς.

3.Όρια Συστήματος: Τα όρια ενός συστήματος καθορίζουν τη διαχωριστική γραμμή ανάμεσα στο σύστημα και το περιβάλλον του, διευκρινίζοντας τον χώρο εντός του οποίου λειτουργεί. [1]

2.2 ΈΝΝΟΙΑ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Ένα Πληροφοριακό Σύστημα (ΠΣ) αποτελείται από έξι κρίσιμα συστατικά, τα οποία συνεργάζονται για την επίτευξη ενός αποδοτικού συστήματος. Αυτά είναι:

Άνθρωποι: Περιλαμβάνει το σύνολο των ατόμων που αλληλοεπιδρούν με το πληροφοριακό σύστημα, ασκώντας διάφορους ρόλους όπως χρήστες, διαχειριστές και τεχνικοί υποστήριξης.

Διαδικασίες: Αφορά το σύνολο των οδηγιών και των διαδικασιών που καθοδηγούν τη χρήση και την αλληλεπίδραση των συστατικών του συστήματος, εξασφαλίζοντας την ορθή λειτουργία και συντονισμό τους.

Βάση Δεδομένων (Database): Αποθηκεύει και διαχειρίζεται τα δεδομένα, παρέχοντας τη βάση για την ανάλυση, την επεξεργασία και την ανάκτηση πληροφοριών.

Λογισμικό (Software): Το σύνολο των προγραμμάτων και των εφαρμογών που εκτελούν συγκεκριμένες λειτουργίες εντός του πληροφοριακού συστήματος.

Υλικός Εξοπλισμός (Hardware): Οι φυσικές συσκευές και εξοπλισμοί που απαιτούνται για την εκτέλεση του λογισμικού και τη διαχείριση των δεδομένων, όπως οι υπολογιστές και οι διακομιστές.

Δίκτυο (Network): Διευκολύνει την επικοινωνία και την ανταλλαγή δεδομένων μεταξύ των διαφόρων συστατικών και χρηστών του συστήματος. [1].

Ένα Πληροφοριακό Σύστημα είναι ουσιώδες για διάφορες λειτουργίες σε οργανισμούς και επιχειρήσεις, καθώς συμβάλλει σημαντικά στον έλεγχο των διεργασιών, στο συντονισμό των δραστηριοτήτων, στην ανάλυση και επίλυση προβλημάτων, στην υποστήριξη λήψης αποφάσεων, και στην ανάπτυξη νέων προϊόντων. Αυτές οι δυνατότητες το καθιστούν

απαραίτητο εργαλείο για την βελτίωση της αποδοτικότητας και της καινοτομίας σε έναν οργανισμό. [1]

Για να λειτουργήσει αποτελεσματικά, κάθε πληροφοριακό σύστημα θα πρέπει:

1. Προσδιορισμός Αναγκών: Να προσδιορίζει με ακρίβεια και αποδοτικότητα τις ανάγκες των χρηστών του, κατανοώντας τις απαιτήσεις και τις προσδοκίες τους από το σύστημα.

2. Επεξεργασία Πληροφοριών: Να επεξεργάζεται και να διαχειρίζεται τις πληροφορίες με τρόπο που να εξασφαλίζει την ορθή και έγκαιρη ικανοποίηση αυτών των αναγκών, βελτιώνοντας έτσι την συνολική λειτουργικότητα του συστήματος. Για να επιτευχθούν οι αναφερθείσες λειτουργίες ενός πληροφοριακού συστήματος με τρόπο που να καλύπτει τις ανάγκες των χρηστών, εφαρμόζονται τα ακόλουθα μέτρα:

1. Αποδοτική Διαχείριση Πληροφοριών:

Εντατικοποίηση της ανάκτησης, αποθήκευσης, επεξεργασίας, παρουσίασης και διάδοσης των πληροφοριών, ώστε να εξασφαλίζεται η υψηλή ποιότητα και η άμεση διαθεσιμότητα των δεδομένων.

2. Ενίσχυση της Μάθησης και Λήψης Αποφάσεων:

Παροχή απαραίτητων εκπαιδευτικών εργαλείων και δημιουργία ενός περιβάλλοντος που ευνοεί την μάθηση, βοηθώντας τους χρήστες να αναπτύξουν καλύτερες δεξιότητες ανάλυσης και λήψης αποφάσεων.

3. Υποστήριξη Οργανωτικών Διαδικασιών:

Ανάπτυξη και βελτίωση των διαδικασιών που σχετίζονται με την λειτουργία, τον έλεγχο και τον στρατηγικό σχεδιασμό της επιχείρησης ή του οργανισμού, ενισχύοντας την ολοκληρωμένη διαχείριση και την αποτελεσματικότητα. [2]

Το ζωτικό κύκλο ενός πληροφοριακού συστήματος περιλαμβάνει τα ακόλουθα βασικά στάδια:

1. Δημιουργία:

Η διαδικασία αρχίζει με την απόφαση της επιχείρησης ή του οργανισμού να αναπτύξει ένα νέο πληροφοριακό σύστημα. Σε αυτό το στάδιο, οι ανάγκες και οι προτεραιότητες είναι προσεκτικά αναγνωρισμένες και καθορίζονται.

2. Σχεδιασμός:

Μετά την κατανόηση των απαιτήσεων, το επόμενο βήμα είναι ο σχεδιασμός του συστήματος. Σε αυτό το στάδιο, οι λειτουργίες που θα ικανοποιήσουν τις απαιτήσεις αυτές αναπτύσσονται και οργανώνονται.

3. Ανάπτυξη και Εξέλιξη:

Κατά τη διάρκεια αυτού του σταδίου, το πληροφοριακό σύστημα υλοποιείται και αναπτύσσεται περαιτέρω. Αυτό περιλαμβάνει την εγκατάσταση, την προσαρμογή και τη

συνεχή βελτίωση του συστήματος ώστε να ανταποκρίνεται στις αλλαγές και τις εξελίξεις της επιχείρησης ή του οργανισμού.

4. Απόσυρση:

Τελικά, όταν το σύστημα δεν είναι πλέον αποδοτικό ή ανταποκρίνεται στις ανάγκες της επιχείρησης, αποσύρεται. Αυτή η απόφαση παίρνεται όταν το κόστος συντήρησης υπερβαίνει τα οφέλη της χρήσης του ή όταν το σύστημα δεν μπορεί να ενσωματώσει νέες τεχνολογίες και απαιτήσεις.

Κάθε ένα από αυτά τα στάδια απαιτεί προσεκτικό σχεδιασμό, συντονισμό και διαχείριση για να διασφαλιστεί ότι το πληροφοριακό σύστημα λειτουργεί αποδοτικά και συνεισφέρει θετικά στις λειτουργίες και στους στόχους της επιχείρησης ή του οργανισμού. Η διαδικασία απόσυρσης του συστήματος πρέπει επίσης να γίνει με τρόπο που να μην επηρεάζει αρνητικά την οργάνωση, εξασφαλίζοντας μια ομαλή μετάβαση σε νέες τεχνολογίες ή συστήματα. [1]

2.2.1 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΕΝΟΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Κάθε πληροφοριακό σύστημα μπορεί να θεωρηθεί ως ένα υποσύστημα ενός ευρύτερου πληροφοριακού συστήματος, ενσωματωμένο σε μια μεγαλύτερη δομή πληροφοριών και λειτουργιών. Αυτή η ενσωμάτωση επιτρέπει την αρμονική αλληλεπίδραση και την αμοιβαία ενίσχυση μεταξύ των διαφόρων υποσυστημάτων, συνεισφέροντας σε μια πιο ενοποιημένη λειτουργία.

Επιπλέον, τα πληροφοριακά συστήματα χαρακτηρίζονται ως ανοιχτά συστήματα, πράγμα που σημαίνει ότι επικοινωνούν και αλληλοεπιδρούν με το εξωτερικό περιβάλλον. Αυτή η ανοιχτή φύση εκδηλώνεται μέσα από διάφορα χαρακτηριστικά, όπως:

Εισαγωγή Ενέργειας: Λαμβάνουν είσοδο ενέργειας σε διάφορες μορφές, είτε ως δεδομένα, είτε ως πόροι από το εξωτερικό περιβάλλον.

Μετασχηματισμός Ενέργειας: Τροποποιούν και επεξεργάζονται την εισερχόμενη ενέργεια για να παράξουν χρήσιμα αποτελέσματα, όπως πληροφορίες και αποφάσεις.

Εξαγωγή Προϊόντος: Εκπέμπουν στο περιβάλλον τα αποτελέσματα της επεξεργασίας τους, είτε ως πληροφορία, είτε ως ενεργειακά προϊόντα.

Κυκλική Ανταλλαγή Δραστηριοτήτων:

Οι διαδικασίες της εισαγωγής, του μετασχηματισμού και της εξαγωγής επαναλαμβάνονται διαδοχικά, δημιουργώντας έναν διαρκή κύκλο λειτουργίας.

Αρνητική Εντροπία:

Αντλούν τάξη από το περιβάλλον τους, αντισταθμίζοντας τη φυσική τάση προς αύξηση της εντροπίας και διατηρώντας την οργανωτική τους δομή.

Διαφοροποίηση και Εξέλιξη:

Προσαρμόζονται και εξελίσσονται βάσει των αρχικών συνθηκών και μέσω διαφορετικών μονοπατιών, οδηγούμενα προς μια κοινή τελική κατάσταση που ανταποκρίνεται στις δυναμικές ανάγκες του περιβάλλοντος. [2]

Αυτά τα χαρακτηριστικά καταδεικνύουν την πολυπλοκότητα και τη δυναμική προσαρμοστικότητα των πληροφοριακών συστημάτων, καθώς και το πώς αυτά αντιδρούν και αλληλοεπιδρούν με το περιβάλλον τους για να παραμένουν αποτελεσματικά και συναφή.

Τα πληροφοριακά συστήματα είναι κρίσιμα για την αποδοτική λειτουργία των επιχειρήσεων και αποτελούνται από πέντε βασικές συνιστώσες: άνθρωποι, δεδομένα, λογισμικό, υλικός εξοπλισμός και διαδικασίες.

1. Άνθρωποι:

Οι χρήστες, οι διαχειριστές, οι τεχνικοί υποστήριξης και άλλοι εμπλεκόμενοι που αλληλοεπιδρούν με το σύστημα.

2. Δεδομένα:

Τα δεδομένα και οι πληροφορίες που εισέρχονται, επεξεργάζονται, αποθηκεύονται και ανακτώνται από το σύστημα.

3. Λογισμικό:

Το σύνολο των προγραμμάτων και εφαρμογών που επεξεργάζονται τα δεδομένα και εκτελούν λειτουργίες.

4. Υλικός Εξοπλισμός:

Οι φυσικές συσκευές και εξοπλισμός, όπως υπολογιστές και διακομιστές, που χρησιμοποιούνται για την εκτέλεση του λογισμικού και την αποθήκευση των δεδομένων.

5. Διαδικασίες: Οι οδηγίες και μέθοδοι που καθορίζουν πώς τα δεδομένα εισάγονται, επεξεργάζονται, αποθηκεύονται και εξάγονται από το σύστημα, ώστε να επιτυγχάνονται οι λειτουργικοί στόχοι. [2]

Η συνεργασία αυτών των πέντε συνιστωσών είναι σημαντική για την αποτελεσματική λειτουργία κάθε πληροφοριακού συστήματος, καθώς αυτό επιτρέπει την ορθή διαχείριση και αξιοποίηση των πληροφοριών σε έναν οργανισμό ή επιχείρηση.

Ένα πληροφοριακό σύστημα προσφέρει ζωτικές υπηρεσίες σε επιχειρήσεις και οργανισμούς, βελτιώνοντας την συνολική λειτουργικότητα και αποδοτικότητα τους. Οι κύριες υπηρεσίες που περιλαμβάνονται είναι:

1. Επεξεργασία Δεδομένων και Πληροφοριών:

Αυτοματοποιεί τη διαχείριση δεδομένων και πληροφοριών, εξασφαλίζοντας την ακρίβεια και την ταχύτητα στην επεξεργασία τους.

2. Υποστήριξη Παραγωγικών και Λειτουργικών Συστημάτων:

Βοηθάει στην ομαλή λειτουργία των παραγωγικών διεργασιών και των λειτουργικών αναγκών της επιχείρησης.

3. Δημιουργία και Διαβίβαση Πληροφοριών:

Παρέχει τα εργαλεία για τη δημιουργία και την έγκυρη διανομή πληροφοριών εντός και εκτός του οργανισμού.

4. Υποβοήθηση Διοίκησης στον Έλεγχο και Λήψη Αποφάσεων:

Ενισχύει τη διοικητική ικανότητα για επίβλεψη και αποφασιστικότητα μέσω προηγμένων αναλυτικών εργαλείων και προσβάσιμων δεδομένων. [2]

Μέσω αυτών των δυνατοτήτων, τα πληροφοριακά συστήματα αποτελούν κεντρικό πυλώνα για την ενίσχυση της αποτελεσματικότητας και της ανταγωνιστικότητας των σύγχρονων επιχειρήσεων και οργανισμών.

Ένα πληροφοριακό σύστημα διακρίνεται για την εγγενώς δυναμική του φύση, αντανακλώντας τις συνεχείς μεταβολές στο περιβάλλον λειτουργίας του και στις σχέσεις μεταξύ των συνιστωσών του (άνθρωποι, δεδομένα, διαδικασίες, υπολογιστές). Αυτές οι μεταβολές αντανακλούν τις διαρκείς αλληλεπιδράσεις με άλλα συστήματα και την εξέλιξη της τεχνολογίας, καθώς και των κοινωνικών απαιτήσεων.

Η ασφάλεια των πληροφοριακών συστημάτων ενισχύεται μέσω δύο δυναμικών δράσεων:

1.Κοινωνική Ενεργοποίηση: Περιλαμβάνει την ενεργή συμμετοχή του κοινωνικού συνόλου και την αξίωση θεσμικής εξασφάλισης των δικαιωμάτων των πολιτών μέσω νομοθετικών μέτρων. Αυτό αντανakλά τη διαδικασία με την οποία τα νομοθετικά όργανα επιδιώκουν να θέσουν τις κατάλληλες νομικές ρυθμίσεις για την προστασία των δεδομένων και τη διαφάνεια των λειτουργιών.

2.Τεχνική Συγκρότηση: Συνίσταται στην καθιέρωση ενός πλαισίου γενικών τεχνικών αρχών και την ανάπτυξη τεχνικών ρυθμίσεων που διασφαλίζουν τη συμμόρφωση των λειτουργούντων πληροφοριακών συστημάτων με τις κυρίαρχες κοινωνικές απόψεις και ανάγκες. Αυτό ενσωματώνει τεχνολογίες και πρακτικές που προσαρμόζονται δυναμικά στις αλλαγές του κοινωνικού και τεχνολογικού περιβάλλοντος.

Αυτές οι δράσεις επιτρέπουν στα πληροφοριακά συστήματα να λειτουργούν αποτελεσματικά και ασφαλώς, ανταποκρινόμενα στις συνεχείς εξελίξεις και τις κοινωνικές απαιτήσεις. [2]

2.3 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΤΟΥ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

2.3.1 Η ΕΝΝΟΙΑ ΤΟΥ ΠΛΗΡΟΦΟΡΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Η έννοια της ασφάλειας ενός πληροφοριακού συστήματος είναι ζωτικής σημασίας και σχετίζεται με την ικανότητα του οργανισμού να προστατεύει τις πληροφορίες του από αλλοιώσεις, καταστροφές και μη εξουσιοδοτημένη πρόσβαση. Αυτό περιλαμβάνει τη διασφάλιση της ορθότητας και της αξιοπιστίας των πληροφοριών που παρέχονται στους εξουσιοδοτημένους χρήστες κατά την αναζήτησή τους. Η διατήρηση της ασφάλειας στηρίζεται σε μέτρα που εξασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και τη συνεχή λειτουργία του συστήματος. [3]

Η ασφάλεια των πληροφοριακών συστημάτων αποτελεί μια διαδικασία που στοχεύει στην προστασία και διατήρηση της λειτουργικότητας των συστημάτων αυτών μέσω τριών βασικών μηχανισμών: πρόληψης, ανίχνευσης και αντίδρασης.

1.Πρόληψη: Αυτό το στοιχείο ασχολείται με την εφαρμογή πολιτικών και τεχνολογικών λύσεων που αποτρέπουν την ανεπιθύμητη ή επιβλαβή παρέμβαση στα συστατικά ενός συστήματος. Περιλαμβάνει τη χρήση φυσικών και λογισμικού εργαλείων όπως τείχη προστασίας, αντιικά προγράμματα, ενημερώσεις ασφαλείας, και διαδικασίες ελέγχου πρόσβασης.

2. Ανίχνευση: Αφορά στην εγκατάσταση συστημάτων που μπορούν να αναγνωρίζουν πότε και πώς προκλήθηκε φθορά στο σύστημα. Αυτό συχνά επιτυγχάνεται μέσω της χρήσης συστημάτων ανίχνευσης εισβολών και συστημάτων διαχείρισης περιστατικών ασφαλείας, τα οποία παρακολουθούν και καταγράφουν τις δραστηριότητες στο δίκτυο και τις εφαρμογές.

3.Αντίδραση:Αυτό το στάδιο ασχολείται με τα μέτρα και τις διαδικασίες που εφαρμόζονται αφότου ανιχνευθεί μια ασφαλιστική παραβίαση, όπως η απομόνωση του προβλήματος, η ανάκτηση των συστατικών και η επαναφορά της λειτουργίας του συστήματος. Επίσης, περιλαμβάνει την αναθεώρηση και βελτίωση των πολιτικών ασφαλείας για να αποτρέπεται η επανάληψη παρόμοιων περιστατικών. [3]

Καθένα από αυτά τα στοιχεία είναι κρίσιμο για την εξασφάλιση της ασφαλούς και απρόσκοπτης λειτουργίας του πληροφοριακού συστήματος, προστατεύοντας τόσο τα δεδομένα όσο και την υποδομή από τις πολυάριθμες απειλές του ψηφιακού κόσμου..

Πολύ καλά παραδείγματα για να απεικονιστεί πώς λειτουργεί η ασφάλεια σε διαφορετικά περιβάλλοντα, τόσο στην καθημερινή ζωή όσο και στον ψηφιακό κόσμο του ηλεκτρονικού εμπορίου. Οι συνιστώσες της ασφάλειας που αναφέρατε (πρόληψη, ανίχνευση, αντίδραση) αποτελούν τη βάση για την κατανόηση των μηχανισμών που συμβάλλουν στην προστασία και τον έλεγχο της ασφάλειας, τόσο στο φυσικό όσο και στο ψηφιακό κόσμο.

Καθημερινή Ζωή

-Πρόληψη:

Η τοποθέτηση κλειδαριών και κάγκελων αποτρέπει προληπτικά την παράνομη είσοδο.

-Ανίχνευση:

Συστήματα συναγερμού και κλειστά κυκλώματα τηλεόρασης ανιχνεύουν παράνομες εισόδους ή δραστηριότητες.

-Αντίδραση:

Η αντίδραση σε περιστατικά με κλήση αστυνομίας και αντικατάσταση κλεμμένων αντικειμένων.

Ηλεκτρονικό Εμπόριο

- Πρόληψη:

Η κρυπτογράφηση δεδομένων προστατεύει τις πληροφορίες κατά τη διάρκεια της διακίνησης.

-Ανίχνευση:

Συστήματα ανίχνευσης απατών εντοπίζουν ασυνήθιστες ή ύποπτες συναλλαγές.

- Αντίδραση:

Ακύρωση συναλλαγών, αλλαγή πιστωτικών καρτών, και ασφαλιστικές διαδικασίες για την αντιμετώπιση των απωλειών.

-Εννοιολογικά Στοιχεία

Οι δύο κύριες συνιστώσες της ασφάλειας, προστασία και έλεγχος, υπογραμμίζουν την ανάγκη για ισορροπημένη προσέγγιση:

- Προστασία: Περιλαμβάνει μέτρα πρόληψης και θεραπείας που στοχεύουν να μειώσουν τις πιθανότητες εμφάνισης ασφαλιστικών περιστατικών.

- Έλεγχος: Στοχεύει στην ανίχνευση και αντίδραση, διασφαλίζοντας ότι τυχόν περιστατικά αντιμετωπίζονται αποτελεσματικά και αποκαθίστανται οι λειτουργίες.

Η συνεχής ενσωμάτωση και ενημέρωση των μέτρων ασφαλείας είναι κρίσιμη για την προστασία τόσο στον φυσικό όσο και στον ψηφιακό κόσμο, προσφέροντας ένα ασφαλές και αξιόπιστο περιβάλλον για χρήστες και επιχειρήσεις.

Είναι σημαντικό να τονιστεί εδώ ότι παρέχοντας έναν γενικό και μονοσήμαντο ορισμό της ασφάλειας πληροφοριακών συστημάτων είναι πολύπλοκο. Στην ανάλυση κάθε συγκεκριμένου πληροφοριακού συστήματος, ο ορισμός πρέπει να καθορίζεται με σαφήνεια από την αρχή. Επιπλέον, όταν κανείς μελετά σχετικά έργα όπως βιβλία ή άρθρα, είναι κρίσιμο να αποδίδεται ιδιαίτερη προσοχή για να αποφευχθεί η δυνατότητα παρερμηνείας του ορισμού της ασφάλειας που χρησιμοποιεί ο συγγραφέας σε σχέση με αυτόν που ενδεχομένως έχουμε εμείς κατά νου. [3]

2.4 ΘΕΜΕΛΙΩΔΗΣ ΕΝΝΟΙΕΣ ΤΟΥ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Σήμερα, είναι κοινώς αποδεκτό ότι η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται άμεσα με τρία κρίσιμα χαρακτηριστικά:

- Εμπιστευτικότητα:

Η προστασία πληροφοριών από μη εξουσιοδοτημένη πρόσβαση και αποκάλυψη.

- Ακεραιότητα:

Η διασφάλιση ότι οι πληροφορίες και τα συστήματα είναι ακέραια και δεν έχουν υποστεί αλλοίωση.

- Διαθεσιμότητα:

Η εξασφάλιση ότι οι χρήστες μπορούν να αξιοποιήσουν τις πληροφορίες ή τους πόρους του συστήματος όποτε χρειάζεται.

Θα προχωρήσουμε στην ανάλυση κάθε μίας από αυτές τις έννοιες, εξετάζοντας την μοναδικότητα και την σημασία τους για τα πληροφοριακά συστήματα ασφαλείας που είναι υπό μελέτη. [3]

2.4.1.ΕΜΠΙΣΤΕΥΤΗΤΙΚΟΤΗΤΑ

Σε πολλά περιστατικά της καθημερινότητας, οι έννοιες της ασφάλειας και της εμπιστευτικότητας είναι συνήθως αλληλένδετες, όπως συμβαίνει σε στρατιωτικά περιβάλλοντα όπου είναι πολύ σημαντικό τα στοιχεία να διατηρούνται μυστικά. Εμπιστευτικότητα ορίζεται ως η προσπάθεια εμποδίστης της μη εξουσιοδοτημένης διαρροής πληροφοριών, δηλαδή της αποτροπής μη εξουσιοδοτημένης πρόσβασης στα δεδομένα. Κατά συνέπεια, αυτό σημαίνει ότι τα δεδομένα που ανταλλάσσονται ή φυλάσσονται σε υπολογιστικά συστήματα είναι προσβάσιμα μόνο από εξουσιοδοτημένα άτομα. Η προστασία αυτή αφορά όχι μόνο την αποφυγή μη εξουσιοδοτημένης αποκάλυψης αυτών των δεδομένων αλλά και την απόκρυψη της ίδιας της ύπαρξης των δεδομένων. Για παράδειγμα, το γεγονός ότι υπάρχει ένας φάκελος εγκληματία μπορεί να είναι εξίσου κρίσιμο με τις λεπτομέρειες του εγκλήματος.

Πρόσθετες διαστάσεις της εμπιστευτικότητας περιλαμβάνουν:

-Ιδιωτικότητα:

Αφορά την προστασία προσωπικών δεδομένων, δηλαδή εκείνων των πληροφοριών που σχετίζονται απευθείας με ατομικά άτομα.

- Μυστικότητα:

.Εστιάζει στην προστασία δεδομένων που είναι ιδιοκτησία ενός οργανισμού, διασφαλίζοντας ότι δεν γίνονται γνωστά εκτός των ορίων του ίδιου του οργανισμού. [3]

2.4.2ΑΚΕΡΑΙΟΤΗΤΑ

Η ακεραιότητα μπορεί γενικά να οριστεί ως η ανάγκη τα πράγματα να λειτουργούν ή να είναι όπως οφείλουν να είναι. Στον τομέα της πληροφορικής, η ακεραιότητα συνδέεται με την προστασία των πληροφοριών από μη εξουσιοδοτημένες τροποποιήσεις, περιλαμβάνοντας την αποτροπή μη εξουσιοδοτημένης εγγραφής, διαγραφής ή δημιουργίας δεδομένων. Κατά συνέπεια, αυτό σημαίνει ότι οι τροποποιήσεις, οι διαγραφές και οι δημιουργίες δεδομένων σε ένα υπολογιστικό σύστημα γίνονται μόνο από εξουσιοδοτημένα μέρη, εξασφαλίζοντας έτσι την ασφάλεια των δεδομένων και παρέχοντας αξιοπιστία στις πληροφορίες που είναι διαθέσιμες στα διάφορα πληροφοριακά συστήματα. [3]

2.4.3 ΔΙΑΘΕΣΙΜΟΤΗΤΑ

Η διαθεσιμότητα αναφέρεται στην ικανότητα πρόσβασης και χρήσης των υπηρεσιών ενός πληροφοριακού συστήματος από εξουσιοδοτημένους χρήστες, χωρίς ανεξήγητες καθυστερήσεις. Αυτό επιτρέπει στους εξουσιοδοτημένους χρήστες να προσπελάσουν τους πόρους του συστήματος χωρίς να αντιμετωπίζουν άρνηση εξυπηρέτησης. Η διαθεσιμότητα ξεπερνά τις παραδοσιακές αντιλήψεις ασφάλειας, απαιτώντας τεχνολογία από άλλους τομείς όπως τον ανεκτικό σε σφάλματα υπολογισμό (fault-tolerant computing). [3]

Για τους σκοπούς ασφάλειας, η κύρια ανησυχία είναι η πρόληψη επιθετικών ενεργειών που στοχεύουν να εμποδίσουν τη νόμιμη πρόσβαση στο σύστημα. Αυτές οι επιθέσεις, γνωστές ως επιθέσεις άρνησης εξυπηρέτησης, επιδιώκουν να διακόψουν την εξουσιοδοτημένη πρόσβαση σε πληροφορίες και πόρους ή να προκαλέσουν καθυστερήσεις σε λειτουργίες που είναι κρίσιμες χρονικά. Οι επιθέσεις αυτές μπορεί να εκδηλωθούν με

τη μορφή «πλημμυρών» στο διαδίκτυο, όπου ο επιτιθέμενος κατακλύζει έναν διακομιστή με αιτήσεις σύνδεσης.

Παρότι η διαθεσιμότητα θεωρείται συχνά ως το κυρίαρχο στοιχείο της ασφάλειας, υπάρχουν σχετικά λίγοι μηχανισμοί που υποστηρίζουν ενεργά αυτή τη λειτουργία. [3]

2.5 ΔΕΥΤΕΡΕΥΟΥΣΕΣ ΕΝΝΟΙΕΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Εκτός από τις βασικές έννοιες της ασφάλειας στα πληροφοριακά συστήματα, υπάρχουν και άλλες δευτερεύουσες έννοιες που είναι επίσης σημαντικές:

1. Εξουσιοδοτημένη χρήση:

Αφορά την εξασφάλιση ότι μόνο τα εξουσιοδοτημένα άτομα έχουν τη δυνατότητα να χρησιμοποιούν το υπολογιστικό σύστημα και τις συνδεδεμένες περιφερειακές συσκευές με τρόπο που έχει προκαθοριστεί.

2. Αυθεντικοποίηση μηνυμάτων:

Σημαίνει την επιβεβαίωση της ταυτότητας του αποστολέα ενός μηνύματος που λαμβάνεται μέσω δικτύου, διασφαλίζοντας ότι το μήνυμα προήλθε πράγματι από τον ισχυριζόμενο αποστολέα.

3. Μη απάρνηση:

Αναφέρεται στη δυνατότητα να επιβεβαιώνεται ότι ένας παραλήπτης έχει πραγματικά λάβει ένα μήνυμα, καθιστώντας αδύνατη την άρνηση της λήψης από πλευράς του.

4. Απόδοση ευθυνών:

Εστιάζει στην αναγκαιότητα των χρηστών να είναι υπεύθυνοι για τις ενέργειές τους. Συνεπώς, απαιτείται ασφαλής ταυτοποίηση χρηστών και διατήρηση λεπτομερών εγγραφών ελέγχου, οι οποίες χρησιμοποιούνται για την επίλυση περιστατικών ασφαλείας και την ενοχοποίηση των υπευθύνων.

5. Αξιοπιστία και σιγουριά:

Αφορά την ανάγκη των συστημάτων να λειτουργούν αξιόπιστα και με ασφάλεια ακόμα και υπό δυσμενείς συνθήκες, όπως στις περιπτώσεις κρίσιμων υποδομών όπως πυρηνικοί σταθμοί και συστήματα ελέγχου αεροπορικής κυκλοφορίας. [3]

2.6 ΠΑΡΑΒΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Οι παραβάσεις ασφαλείας σε υπολογιστικά συστήματα συνδέονται με τέσσερις κύριες έννοιες: έκθεση, ευπάθεια, απειλή και χειρισμός, ως εξής:

1. **Έκθεση**: Συνεπάγεται την πιθανότητα των δεδομένων να αποκαλυφθούν, να τροποποιηθούν, ή να εμποδιστεί η νόμιμη πρόσβαση σε αυτά για υπολογιστικές διεργασίες. Παραδείγματα περιλαμβάνουν:
 - Μη εξουσιοδοτημένη αποκάλυψη δεδομένων
 - Μη εξουσιοδοτημένη τροποποίηση δεδομένων
 - Άρνηση νόμιμης πρόσβασης σε υπολογιστικούς πόρους
2. **Ευπάθεια**: Αναφέρεται σε μια αδυναμία στο σύστημα ασφαλείας που μπορεί να εκμεταλλευτεί κάποιος για να προκαλέσει απώλειες ή ζημιές.
3. **Απειλή**: Είναι η πιθανότητα να συμβεί κάτι που θα προκαλέσει απώλειες ή ζημιές στο σύστημα. Παραδείγματα απειλών περιλαμβάνουν:
 - Ανθρώπινες επιθέσεις
 - Φυσικές καταστροφές
 - Ακούσια ανθρώπινα λάθη
 - Εσωτερικές ατέλειες του εξοπλισμού ή του λογισμικού
4. **Χειρισμός ή Έλεγχος**: Περιλαμβάνει την υλοποίηση μέτρων που μειώνουν τις ευπάθειες του συστήματος, ενισχύοντας την προστασία και μειώνοντας τις Πιθανότητες εκμετάλλευσης των ευπαθειών.

Οι κύριες απειλές στην ασφάλεια ενός υπολογιστικού συστήματος περιλαμβάνουν διακοπή, μεταβολή, υποκλοπή και παραποίηση. Ειδικότερα:

- Η διακοπή προκύπτει όταν ένα συστατικό του συστήματος γίνεται απρόσιτο ή χάνεται.
- Η μεταβολή σημαίνει ότι ένα μη εξουσιοδοτημένο άτομο, έχοντας αποκτήσει πρόσβαση, τροποποιεί ένα στοιχείο του συστήματος.
- Η υποκλοπή αναφέρεται στην πρόσβαση σε συστατικά του συστήματος από μη εξουσιοδοτημένα άτομα.
- Η παραποίηση εμφανίζεται όταν κάποιος μη εξουσιοδοτημένος παραχαράσσει δεδομένα ή συστατικά ενός υπολογιστικού συστήματος. [3]

2.7 Ευπάθειες Πληροφοριακών Συστημάτων

Κάθε Πληροφοριακό Σύστημα (ΠΣ) κινδυνεύει από επιθέσεις, αλλά η ενσωμάτωση ορισμένων πολιτικών ασφαλείας και η χρήση εξειδικευμένων προϊόντων ασφαλείας μπορεί να μειώσει σημαντικά την πιθανότητα επιτυχίας των επιθέσεων. Αυτά τα μέτρα αυξάνουν το κόστος και το χρονικό διάστημα που απαιτείται για μια επίθεση, κάνοντας την προσπάθεια των εισβολέων απαγορευτική. Παρ' όλα αυτά, είναι κρίσιμο να κατανοήσουμε ότι πλήρης ασφάλεια δεν είναι εφικτή και κανένα σύστημα δεν μπορεί να είναι απόλυτα ασφαλές.

Οι κύριες κατηγορίες ευπαθειών στα πληροφοριακά συστήματα περιλαμβάνουν:

1. **Φυσικές ευπάθειες:** Προβλήματα που σχετίζονται με τη φυσική τοποθεσία και την προστασία των συσκευών.
2. **Ευπάθειες από φυσικά αίτια:** Ζημιές από φυσικά φαινόμενα όπως σεισμοί, πλημμύρες ή καταιγίδες.
3. **Ευπάθειες σε υλικό και λογισμικό:** Τεχνικά προβλήματα ή παραλείψεις στην κατασκευή ή στον προγραμματισμό.
4. **Ευπάθειες μέσων:** Ζημιές στα μέσα αποθήκευσης και μετάδοσης δεδομένων.
5. **Ευπάθειες από εκπομπές:** Κίνδυνοι από ακούσιες εκπομπές που μπορεί να ανιχνευτούν από μακριά.
6. **Ευπάθειες στις επικοινωνίες:** Κίνδυνοι στη μετάδοση δεδομένων μεταξύ συστημάτων.
7. **Ανθρώπινες ευπάθειες:** Λάθη ή εσκεμμένες πράξεις από τους χρήστες του συστήματος.

Στις ακόλουθες ενότητες, θα αναλυθούν αυτές οι ευπάθειες των πληροφοριακών συστημάτων πιο αναλυτικά, εξετάζοντας τους κινδύνους και τις στρατηγικές προστασίας για κάθε κατηγορία.

2.7.1 . ΦΥΣΙΚΕΣ ΕΥΠΑΘΕΙΕΣ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Αναφέρονται στο 'φυσικό περιβάλλον', όπως είναι τα κτίρια και οι χώροι των μηχανογραφικών κέντρων (computer rooms). Η πρώτη γραμμή άμυνας ενάντια σε πιθανές εισβολές περιλαμβάνει τα κλασικά μέσα προστασίας, όπως τον έλεγχο φυσικής προσπέλασης με τη χρήση φυλάκων, βιομετρικών συσκευών, αντικλεπτικών συναγερμών και άλλων μέτρων ασφαλείας.

2.7.2 ΕΚ ΦΥΣΕΩΣ ΕΥΠΑΘΕΙΕΣ

Οι υπολογιστές είναι ιδιαίτερα ευάλωτοι σε φυσικές καταστροφές και περιβαλλοντικές απειλές, όπως πυρκαγιές, πλημμύρες, σεισμοί, κεραυνοί και διακοπές ηλεκτρικού ρεύματος. Επιπλέον, επηρεάζονται αρνητικά από συνθήκες όπως η σκόνη, η υγρασία και οι ακραίες θερμοκρασίες.

2.7.3 ΕΥΠΑΘΕΙΕΣ ΥΛΙΚΟΥ ΚΑΙ ΛΟΓΙΣΜΙΚΟΥ

Διαταραχές στο υλικό και σφάλματα στο λογισμικό μπορούν να προκαλέσουν διακοπή στις υπηρεσίες ενός Πληροφοριακού Συστήματος (ΠΣ), είτε λόγω ενδογενών ελαττωμάτων είτε λόγω λανθασμένης τοποθέτησης των συστατικών του.

2.7.4 ΕΥΠΑΘΕΙΕΣ ΜΕΣΩΝ

Η απώλεια ή η καταστροφή μαγνητικών μέσων και εκτυπωμένων υλικών μπορεί να οδηγήσει στη διαρροή ή στην απώλεια ευαίσθητων δεδομένων.

2.7.5 ΕΥΠΑΘΕΙΕΣ ΕΚΠΟΜΠΩΝ

Η ηλεκτρομαγνητική ακτινοβολία που εκπέμπεται από ηλεκτρονικές συσκευές μπορεί να υποκλαπεί με τη χρήση κατάλληλου εξοπλισμού, επιτρέποντας την αποκωδικοποίηση των σημάτων για την κλοπή κρίσιμων πληροφοριών ή για την παρεμπόδιση της λειτουργίας του συστήματος.

2.7.6 ΕΥΠΑΘΕΙΕΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

Η σύνδεση του υπολογιστή σε ανοικτά δίκτυα όπως το διαδίκτυο αυξάνει τον κίνδυνο επιθέσεων από μη εξουσιοδοτημένα μέρη. Τα δεδομένα μπορεί να υποκλαπούν, να παραποιηθούν ή να αλλάξουν διαδρομή, και οι γραμμές σύνδεσης είναι συχνά στόχοι για παρεμβάσεις.

2.7.7 ΑΝΘΡΩΠΙΝΕΣ ΕΥΠΑΘΕΙΕΣ

Οι άνθρωποι που διαχειρίζονται και χρησιμοποιούν το Πληροφοριακό Σύστημα αποτελούν συχνά τη μεγαλύτερη πηγή ευπαθειών. Η ανεπαρκής εκπαίδευση, η απροσεξία και οι δόλιες πράξεις, όπως η κακή χρήση συνθηματικών ή άλλων ευαίσθητων στοιχείων, καθώς και οι δυσανεστημένοι υπάλληλοι μπορεί να αποτελέσουν σοβαρές απειλές. [3]

2.8 ΑΠΕΙΛΕΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Όπως έχει επισημανθεί στα προηγούμενα κεφάλαια, τα πληροφοριακά συστήματα αντιμετωπίζουν απειλές που ενδέχεται να προκαλέσουν απώλειες ή ζημιές. Αυτές οι απειλές ανήκουν στα πλέον δυσμενή γεγονότα με τα οποία μπορεί να έρθει αντιμέτωπο ένα λογισμικό σύστημα. Θα προχωρήσουμε στην ανάλυση αυτών των απειλών.

2.8.1 Είδη Απειλών Πληροφοριακών Συστημάτων

Αναλυτικά, σχετικά με τα βασικά συστατικά ενός πληροφοριακού συστήματος, δηλαδή το υλικό (hardware), το λογισμικό (software), και τα δεδομένα (data), διακρίνουμε τις εξής κατηγορίες απειλών:

1.Υποκλοπή (Interception): Κάποιο μη εξουσιοδοτημένο μέρος καταφέρνει να αποκτήσει πρόσβαση σε κάποιο τμήμα του συστήματος. Παραδείγματα περιλαμβάνουν την κλοπή υλικού ή λογισμικού, την αντιγραφή αρχείων χωρίς άδεια, και την παράνομη παρακολούθηση δικτυακής κίνησης για πρόσβαση σε δεδομένα που μεταδίδονται. Αυτή η απειλή αφορά κυρίως την εμπιστευτικότητα του συστήματος.

2. Μεταβολή (Modification): Κάποιο μη εξουσιοδοτημένο μέρος δεν περιορίζεται στην απλή πρόσβαση, αλλά παραποιεί λογισμικό ή δεδομένα. Παραδείγματα περιλαμβάνουν την τροποποίηση ενός προγράμματος με έναν ιό ή την αλλαγή δεδομένων σε μια βάση δεδομένων. Αυτή η απειλή στοχεύει κυρίως την ακεραιότητα του συστήματος.

3. Πλαστογραφία (Fabrication): Αυτή η απειλή εστιάζεται αποκλειστικά στα δεδομένα του συστήματος και συμβαίνει όταν ένα μη εξουσιοδοτημένο μέρος εισάγει παραποιημένα δεδομένα. Παραδείγματα περιλαμβάνουν την εισαγωγή πλαστών συναλλαγών σε ένα τραπεζικό σύστημα ή την επανάληψη μηνυμάτων για την παραπλάνηση του συστήματος. Αυτή η απειλή επηρεάζει την ακεραιότητα και τη διαθεσιμότητα.

4. Διακοπή (Interruption): Ένα τμήμα του συστήματος γίνεται μη διαθέσιμο ή χάνεται εντελώς. Παραδείγματα περιλαμβάνουν τη διαγραφή προγραμμάτων ή αρχείων, ή την εσκεμμένη καταστροφή υλικού. Αυτή είναι κυρίως μια απειλή κατά της διαθεσιμότητας του συστήματος. Ο όρος "άρνηση εξυπηρέτησης" (denial of service) συχνά περιγράφει μια επιτυχημένη επίθεση αυτού του είδους. [3]

2.9 Κατηγορίες Απειλών

Βάσει της προέλευσης τους, οι απειλές σε ένα πληροφοριακό σύστημα μπορούν να καταταχθούν στις εξής τρεις βασικές κατηγορίες:

1. **Φυσικές Απειλές:** Περιλαμβάνουν καταστροφές όπως πυρκαγιά, πλημμύρα κ.ά., τις οποίες δεν είναι πάντα δυνατόν να αποτρέψουμε. Είναι όμως κρίσιμο να ανιχνεύονται έγκαιρα για να μειώνονται οι πιθανότητες σοβαρών ζημιών και να αποφεύγονται δράσεις που ενδεχομένως θα αύξαναν την πιθανότητα της εκδήλωσής τους. Η χρήση εφεδρικών συστημάτων και η τακτική δημιουργία αντιγράφων ασφαλείας για κρίσιμα δεδομένα μπορούν να περιορίσουν τις αρνητικές συνέπειες.
2. **Ακούσιες Απειλές:** Προέρχονται από σφάλματα στο υλικό ή το λογισμικό (HW/SW failures), ή από την άγνοια ή την αδιαφορία του ανθρώπινου παράγοντα. Η έλλειψη κατάλληλης εκπαίδευσης τόσο για τους απλούς χρήστες όσο και για τους διαχειριστές των συστημάτων αποτελεί έναν σημαντικό παράγοντα που μπορεί να προκαλέσει τέτοιες απειλές. Σημειώνεται ότι η αγνοία είναι πιο συχνά αιτία προβλημάτων από την κακή πρόθεση.
3. **Εκούσιες Απειλές:** Αυτές οι απειλές τραβούν συνήθως την μεγαλύτερη δημοσιότητα και περιλαμβάνουν κακόβουλες δράσεις από εσωτερικούς χρήστες, όπως δυσανεκτικοί υπάλληλοι, αλλά και από επίδοξους εξωτερικούς εισβολείς. Η επιτυχία των επιθέσεων εξαρτάται συνήθως από τους πόρους που διαθέτουν οι δράστες, όπως χρόνος, υπολογιστική ισχύς, γνώσεις, ανθρώπινο δυναμικό, χρήματα, συσκευές και εξαρτήματα. Οι εκούσιες απειλές μπορεί να αναζητούν

εκδίκηση, οικονομικό κέρδος, αναγνώριση, ή απλώς να προκαλέσουν προβλήματα και να διαπράξουν βανδαλισμούς. [3]

2.10 Μέτρα Προστασίας Πληροφοριακού Συστήματος

Τα μέτρα προστασίας ή αντίμετρα αποτελούν τις διαδικασίες, τεχνικές, ενέργειες και συσκευές που χρησιμοποιούνται για να μειώσουν τις ευπάθειες ενός Πληροφοριακού Συστήματος (ΠΣ). Αυτά τα μέτρα μπορούν να κατανεμηθούν στις ακόλουθες βασικές συνιστώσες ασφάλειας:

1. Φυσική Ασφάλεια Συστήματος (Physical Security): Αφορά την προστασία του φυσικού εξοπλισμού από φυσικές απειλές όπως κλοπή, βανδαλισμοί, πλημμύρες και φωτιά. Η εγκατάσταση συστημάτων συναγερμού και οι φυσικοί φραγμοί είναι παραδείγματα μέτρων που υιοθετούνται.

2. Ασφάλεια Υπολογιστικού Συστήματος (Computer Security):

Επικεντρώνεται στην προστασία των πληροφοριών που διαχειρίζεται το λειτουργικό σύστημα, όπως εφαρμογές και αρχεία δεδομένων. Τα μέτρα περιλαμβάνουν τον περιορισμό της πρόσβασης στα δεδομένα και τις εφαρμογές μέσω της χρήσης δικαιωμάτων και πολιτικών ασφαλείας.

3. Ασφάλεια Βάσεων Δεδομένων (Database Security): Στοχεύει στην εφαρμογή ενός προκαθορισμένου πλαισίου πολιτικής για την προστασία των περιεχομένων μιας βάσης δεδομένων. Καθορίζει ποιοι έχουν το δικαίωμα να προβαίνουν σε προβολή ή τροποποίηση των προστατευμένων δεδομένων.

4. Ασφάλεια Δικτύων Επικοινωνιών (Network Security):* Προστατεύει τις πληροφορίες κατά την μετάδοση μέσω δικτυακών καναλιών, όπως τηλεφωνικά, δορυφορικά, ή άλλα δίκτυα επικοινωνίας. Περιλαμβάνει τη χρήση κρυπτογραφίας, την ασφαλή διαμόρφωση δικτυακών συσκευών, και την εφαρμογή πολιτικών ασφαλείας για τον έλεγχο της πρόσβασης και της ταυτοποίησης. [3]

2.10.1 Κατηγορίες Μέτρων Ασφαλείας

Υπάρχουν τέσσερις βασικοί τρόποι άμυνας που συμβάλλουν στην ενίσχυση της ασφάλειας ενός πληροφοριακού συστήματος (ΠΣ):

1. Μέτρα Προσπέλασης Συστήματος: Αυτά τα μέτρα διασφαλίζουν ότι μη εξουσιοδοτημένοι χρήστες δεν μπορούν να συνδεθούν (log in) στο σύστημα. Περιλαμβάνουν τεχνολογίες όπως ταυτοποίηση διαπιστευτηρίων, διαδικασίες ελέγχου ταυτότητας και άλλα μέτρα ασφαλείας στην πρόσβαση.

2. Μέτρα Προσπέλασης Δεδομένων: Καθορίζουν ποιος μπορεί να έχει πρόσβαση σε ποια δεδομένα και για ποιον σκοπό. Οι εφαρμογές βάσεων δεδομένων, για παράδειγμα, απαιτούν λεπτομερή ελέγχους πρόσβασης για να εξασφαλίσουν ότι τα δεδομένα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση.

3. Διαχείριση Συστήματος και Ασφάλειας: Περιλαμβάνει την εκτέλεση διαδικασιών offline που διαμορφώνουν ή επιβάλλουν ασφαλή περιβάλλοντα, ορίζοντας σαφώς τις υπευθυνότητάς του διαχειριστή του συστήματος, παρέχοντας εκπαίδευση στους χρήστες και διασφαλίζοντας ότι οι διαδικασίες ασφαλείας τηρούνται σωστά.

4. Σχεδιασμός Συστήματος: Εκμεταλλεύεται τα βασικά χαρακτηριστικά και τις δυνατότητες ασφαλείας του υλικού και του λογισμικού, προσαρμόζοντας το σύστημα για να ενισχύσει την γενική ασφάλεια και να ενσωματώσει άμυνες σε κάθε επίπεδο της αρχιτεκτονικής του. [3]

2.10.2 Τύποι Μέτρων Ασφαλείας Πληροφοριακού Συστήματος

Για την προστασία ενός πληροφοριακού συστήματος από τις διάφορες απειλές και την εκμετάλλευση των ευπαθειών του, υπάρχουν πολλά είδη μέτρων ασφαλείας:

1. Κρυπτογράφηση (Encryption): Μετατρέπει τα δεδομένα σε μη αναγνώσιμη μορφή για οποιονδήποτε δεν διαθέτει το κλειδί, εξαλείφοντας έτσι την αξία των υποκλοπών και μειώνοντας δραστικά την πιθανότητα ανεπιθύμητων τροποποιήσεων.

2. Μέτρα Λογισμικού (Software Controls): Τα λογισμικά θα πρέπει να σχεδιάζονται με ασφάλεια, να είναι αξιόπιστα και να αποτρέπουν εξωτερικές επιθέσεις, εξασφαλίζοντας ότι προγράμματα και δεδομένα είναι καλά προστατευμένα.

3. Μέτρα Ανάπτυξης (Development Controls):

Αφορά τα πρότυπα ανάπτυξης, κωδικοποίησης, ελέγχου και συντήρησης του λογισμικού, ενισχύοντας την ασφαλή λειτουργία των προγραμμάτων.

4. Μέτρα Λειτουργικού Συστήματος (Operating System Controls):

Περιλαμβάνουν περιορισμούς και πολιτικές που επιβάλλονται από το λειτουργικό σύστημα για να προστατεύσουν τους χρήστες από αλληλοεπεμβάσεις.

5. Μέτρα εντός των Προγραμμάτων (Internal Program Controls):

Πρόκειται για την ενσωμάτωση μηχανισμών ασφαλείας εντός των ίδιων των προγραμμάτων, όπως περιορισμοί πρόσβασης σε συστήματα διαχείρισης βάσεων δεδομένων.

6. Μέτρα Υλικού (Hardware Controls):

Ποικίλλουν από την υλοποίηση της κρυπτογράφησης σε υλικό μέχρι τις συσκευές επιβεβαίωσης ταυτότητας χρηστών, παρέχοντας αυξημένα επίπεδα φυσικής και τεχνολογικής ασφαλείας.

7. Φυσικά Μέτρα Υλικού (Physical Hardware Controls):

Απλά και αποτελεσματικά μέτρα όπως κλειδαριές, φύλακες, και αντίγραφα ασφαλείας ενισχύουν την ασφάλεια των φυσικών εξαρτημάτων του συστήματος.

8. Πολιτικές Ασφάλειας (Security Policies):

Οι πολιτικές και οι διαδικασίες ελέγχου προσπέλασης προσαρμόζονται στις ανάγκες και στις συνθήκες ασφαλείας του κάθε πληροφοριακού συστήματος, εξασφαλίζοντας ότι όλοι οι χρήστες και διαχειριστές ακολουθούν τις κατάλληλες διαδικασίες. [3]

2.11 Αποτελεσματικότητα Μέτρων Ασφαλείας

Η αποτελεσματικότητα των μέτρων προστασίας ή αντίμετρων εξαρτάται σημαντικά από το πόσο σωστά εφαρμόζονται και διαχειρίζονται. Κρίσιμοι παράγοντες που επηρεάζουν αυτήν την αποτελεσματικότητα περιλαμβάνουν:

1. Επίγνωση του Προβλήματος:

Τα άτομα που υλοποιούν ή σχεδιάζουν τα μέτρα ασφαλείας πρέπει να είναι πλήρως ενημερωμένα για τη σημασία και την ανάγκη της ασφάλειας. Η σωστή κατανόηση του προβλήματος εξασφαλίζει ότι τα μέτρα θα είναι στοχευμένα και θα καλύπτουν τις συγκεκριμένες ανάγκες ασφαλείας.

2. Περιοδικές Αναθεωρήσεις:

Ο δυναμικός χαρακτήρας των πληροφοριακών συστημάτων και των περιβαλλόντων στα οποία λειτουργούν απαιτεί τακτική επανεξέταση και ανανέωση των μέτρων ασφαλείας. Το συνεχές μοντέλο αναθεώρησης εγγυάται ότι τα μέτρα παραμένουν επίκαιρα και αποτελεσματικά αντιμετωπίζοντας νέες απειλές και ευπάθειες.

3. Αλληλοεπικάλυψη Μέτρων: Η αποτελεσματική αντιμετώπιση των ευπαθειών συχνά απαιτεί τη συνδυαστική εφαρμογή διαφορετικών μέτρων ασφαλείας. Ένας συνδυασμός φυσικών, υπολογιστικών, και δικτυακών μέτρων μπορεί να μειώσει σημαντικά τις υπάρχουσες απειλές. Η συνολική ασφάλεια του συστήματος συχνά εξαρτάται από την ικανότητα των διαφορετικών μέτρων να συμπληρώνουν το ένα το άλλο, βελτιώνοντας την ασφάλεια πέραν των αντοχών κάθε μεμονωμένου μέτρου.

Αυτοί οι παράγοντες καθορίζουν το πόσο αποτελεσματικά θα λειτουργήσει ένα σύστημα ασφαλείας, υπογραμμίζοντας τη σημασία της ενημέρωσης, της ευελιξίας και της συνεργασίας μεταξύ των διάφορων μέτρων. Όπως τονίζεται, η αλυσίδα της ασφάλειας είναι τόσο δυνατή όσο ο αδυνατότερος κρίκος της, επομένως κάθε μέρος του συστήματος πρέπει να λαμβάνει τη δέουσα προσοχή. [3]

2.11.1 Τοποθέτηση Μέτρων Ασφαλείας σε Πληροφοριακό Σύστημα

Για την αποτελεσματική προστασία ενός πληροφοριακού συστήματος (ΠΣ), τα μέτρα ασφαλείας μπορούν να εφαρμοστούν σε διάφορα στρώματα του συστήματος. Ένα τυπικό ΠΣ μπορεί να αναλυθεί στα εξής πέντε στρώματα:

1. Προγράμματα Εφαρμογών: Τα ειδικά σχεδιασμένα προγράμματα που ικανοποιούν τις απαιτήσεις των χρηστών. Μέτρα ασφαλείας εδώ μπορεί να περιλαμβάνουν την κρυπτογράφηση δεδομένων και την ασφάλεια σε επίπεδο εφαρμογής, όπως την επαλήθευση ταυτότητας και τον έλεγχο πρόσβασης.

2. Υπηρεσίες: Αφορούν στοιχεία που χρησιμοποιούνται από τα προγράμματα εφαρμογών, όπως Συστήματα Διαχείρισης Βάσεων Δεδομένων ή κατακευκτωμένα συστήματα αρχείων. Εδώ, τα μέτρα μπορεί να περιλαμβάνουν τη διαχείριση πρόσβασης στις βάσεις δεδομένων και την εφαρμογή πολιτικών ασφαλείας στα δεδομένα.

3. Λειτουργικό Σύστημα: Παρέχει τις βασικές υπηρεσίες στο σύστημα, όπως διαχείριση αρχείων και εκτυπωτών. Μέτρα σε αυτό το στρώμα περιλαμβάνουν την προστασία του κώδικα του λειτουργικού συστήματος και την επιβολή πολιτικών ασφαλείας που αποτρέπουν την παράνομη πρόσβαση ή την τροποποίηση κρίσιμων διαδικασιών.

4. Πυρήνας: Το κεντρικό τμήμα του λειτουργικού συστήματος, ρυθμίζει την πρόσβαση στη μνήμη και τον επεξεργαστή. Μέτρα εδώ μπορεί να αφορούν την ασφάλεια σε επίπεδο πυρήνα, προστατεύοντας κρίσιμες λειτουργίες του συστήματος από επιθέσεις ή κακόβουλες αλλαγές.

5. Υλικό (Hardware): Αφορά τα φυσικά συστατικά όπως επεξεργαστές και μνήμη. Μέτρα εδώ περιλαμβάνουν φυσική ασφάλεια, κρυπτογράφηση σε επίπεδο υλικού, και συσκευές ασφαλείας που ελέγχουν την πρόσβαση στο φυσικό εξοπλισμό.

Η σωστή τοποθέτηση και εφαρμογή αυτών των μέτρων ασφαλείας σε κάθε ένα από τα στρώματα του πληροφοριακού συστήματος είναι κρίσιμη για την ολοκληρωμένη προστασία του. Κάθε στρώμα απαιτεί εξειδικευμένα μέτρα που συμβάλλουν στην αποτροπή, αντιμετώπιση και ανάκτηση από διάφορους τύπους απειλών και επιθέσεων.

Οι μηχανισμοί ασφαλείας στα στρώματα που βρίσκονται πλησιέστερα στο υλικό τείνουν να είναι πιο γενικευμένοι και επικεντρωμένοι στις λειτουργίες του υπολογιστή (computer-oriented), ενώ εκείνοι που βρίσκονται κοντύτερα στις εφαρμογές είναι σχεδιασμένοι να εξυπηρετούν κυρίως τις ανάγκες των χρηστών (user-oriented). [3]

2.11.2 Απαιτήσεις Ασφαλείας Πληροφοριακών Συστημάτων

Ο πρωταρχικός στόχος της ασφάλειας σε πληροφοριακά συστήματα είναι η προστασία του συνόλου των συστημάτων υπολογιστών και όλων των συναφών στοιχείων (όπως ο ίδιος ο υπολογιστής, οι εγκαταστάσεις, οι χώροι εργασίας, το δίκτυο καλωδιώσεων και τα μέσα αποθήκευσης). Επίσης, μια σημαντική προτεραιότητα είναι η προστασία των πληροφοριών που αποθηκεύονται στα συστήματα. Ενδιαφέρον επίσης παρουσιάζει το γεγονός ότι οι απειλές δεν προέρχονται μόνο από μη εξουσιοδοτημένα άτομα, όπως επισκέπτες σε μια δημόσια υπηρεσία, αλλά και από εξουσιοδοτημένους χρήστες ή ακόμα και διαχειριστές συστημάτων, οι οποίοι μπορεί να επιδιώξουν να πραγματοποιήσουν μη εξουσιοδοτημένες ενέργειες. Αυτό καταδεικνύει την ανάγκη για σύστημα πληροφορικής που να είναι σε θέση να προσφέρει αδιάσειστες αποδείξεις για τις ενέργειες ενός ατόμου, ενισχύοντας την απόδοση ευθυνών.

2.11.3 Ασφάλεια των Πληροφοριών στο Διαδίκτυο

Η διακίνηση δεδομένων μέσω του διαδικτύου προσφέρει σημαντικά οφέλη σε σύγκριση με τις παραδοσιακές μεθόδους. Τα δεδομένα είναι αμέσως διαθέσιμα για χρήση και εκμετάλλευση, ανεξαρτήτως όγκου, ενώ το κόστος αποστολής, ανεξαρτήτως απόστασης, είναι εξαιρετικά χαμηλό. Ωστόσο, η χρήση του διαδικτύου εισάγει επιπλέον απειλές για την ασφάλεια των πληροφοριών. Επιπρόσθετα, οι συνδεδεμένοι στο διαδίκτυο υπολογιστές μπορεί να είναι στόχοι διαφόρων επιθέσεων. Για την ασφαλή διακίνηση δεδομένων μέσω διαδικτύου, θα πρέπει να διασφαλίζεται ότι:

1. Τα δεδομένα δεν είναι αναγνώσιμα ή αναγνωρίσιμα από κανέναν εκτός από τον αποστολέα και τον παραλήπτη.
2. Τα δεδομένα δεν αλλοιώνονται κατά τη μεταφορά τους μέσω του διαδικτύου, δηλαδή το μήνυμα που παραλαμβάνεται είναι ίδιο με αυτό που αποστέλλεται.
3. Ο αποστολέας και ο παραλήπτης είναι πραγματικά οι άτομα που ισχυρίζονται ότι είναι.
4. Ο αποστολέας δεν μπορεί να αρνηθεί την αποστολή ενός μηνύματος.
5. Οι εμπιστευτικές πληροφορίες προστατεύονται από μη εξουσιοδοτημένη αποκάλυψη.
6. Οι υπολογιστές προστατεύονται από ιούς που μεταδίδονται μέσω του διαδικτύου.

7. Οι ευαίσθητες πληροφορίες, όπως αριθμοί πιστωτικών καρτών και άλλα προσωπικά δεδομένα, προστατεύονται επαρκώς κατά τη διακίνησή τους μέσω του διαδικτύου, για παράδειγμα μέσω κατάλληλης κρυπτογράφησης. [3]

2.11.4 Προκλήσεις στην Εισαγωγή Μηχανισμών Ασφάλειας σε Ένα Πληροφοριακό Σύστημα

Η ενσωμάτωση μηχανισμών ασφαλείας σε ένα πληροφοριακό σύστημα (ΠΣ) αντιπροσωπεύει μία σημαντική και συχνά περίπλοκη διαδικασία. Οι κύριες προκλήσεις που εμπλέκονται σε αυτή τη διαδικασία περιλαμβάνουν:

1. Πολυπλοκότητα του Λογισμικού:

Τα σύγχρονα πληροφοριακά συστήματα συχνά περιλαμβάνουν εκτεταμένο και πολύπλοκο λογισμικό, το οποίο μπορεί να καταστεί δύσκολο να υλοποιηθεί χωρίς την εμφάνιση σφαλμάτων.

2. Μεταγενέστερη Προσθήκη Ασφάλειας:

Συχνά, τα μέτρα ασφαλείας δεν περιλαμβάνονται στο αρχικό σχεδιασμό ή υλοποίηση του συστήματος αλλά προστίθενται αργότερα, κάτι που μπορεί να δυσκολέψει την ολοκληρωμένη και αποτελεσματική ενσωμάτωσή τους.

3. Κόστος Ασφάλειας:

Η υλοποίηση αποτελεσματικών μέτρων ασφαλείας συχνά συνεπάγεται σημαντικό οικονομικό κόστος, τόσο για την αγορά του απαιτούμενου εξοπλισμού και λογισμικού όσο και για τη συντήρηση και διαχείριση του συστήματος.

4. Ανθρώπινος Παράγοντας:

Πολλές φορές το πρόβλημα ασφαλείας δεν προκύπτει από την τεχνολογία καθαυτή αλλά από τους χρήστες που την χρησιμοποιούν. Είτε λόγω έλλειψης κατάλληλης κατάρτισης είτε λόγω εσκεμμένων παραβιάσεων, οι άνθρωποι μπορούν να αποτελέσουν μια μεγάλη απειλή για την ασφάλεια του συστήματος.

Η κατανόηση και αντιμετώπιση αυτών των προβλημάτων είναι κρίσιμη για την ασφαλή και αποτελεσματική λειτουργία των πληροφοριακών συστημάτων στον σύγχρονο ψηφιακό κόσμο. [3]

2.11.5 Αναγκαιότητα και Σκοπιμότητα της Ασφάλειας σε Πληροφοριακά Συστήματα

Παρόλο που η αξία της ασφαλείας είναι αδιαμφισβήτητη, η υιοθέτηση των απαραίτητων μέτρων ασφαλείας συχνά φέρει πρόσθετο βάρος στην απόδοση και το κόστος λειτουργίας του πληροφοριακού συστήματος ενός οργανισμού. Η ασφάλεια πρέπει να θεωρηθεί ως ένα απαραίτητο κόστος, τόσο σε χρόνο όσο και σε χρήμα, για την ομαλή και απρόσκοπτη

λειτουργία του συστήματος. Η επένδυση στην ασφάλεια πρέπει να θεωρείται στρατηγική επιλογή που εξισορροπεί το κόστος εισαγωγής των μέτρων ασφάλειας με το κόστος που θα προκύψει από πιθανές ζημιές λόγω ασφαειακών παραβιάσεων. Αυτή η στρατηγική πρέπει να σχεδιάζει συνθήκες ασφάλειας που δεν θα εμποδίζουν την ευελιξία και την ανάπτυξη του οργανισμού.

Η συγκεκριμένη πολιτική ασφάλειας προκύπτει από μια δυναμική αξιολόγηση του κόστους των μέτρων ασφάλειας σε σχέση με τις πιθανές συνέπειες από ένα ασφαειακό περιστατικό. Είναι ζωτικής σημασίας οι αποφάσεις για τη λήψη ασφαειακών μέτρων να βασίζονται στην αναλογία πιθανότητας εμφάνισης ενός περιστατικού και τις αντίστοιχες συνέπειες. Όταν το αναμενόμενο κόστος των συνεπειών υπερβαίνει το κόστος προληπτικών μέτρων, τα μέτρα ασφάλειας γίνονται αναγκαία.

Η ασφάλεια διατηρεί μια δυναμική φύση, αλλάζοντας συνεχώς λόγω τεχνολογικών εξελίξεων, αυξανόμενης πολυπλοκότητας των συστημάτων και εξελισσόμενων απειλών, απαιτώντας τακτική επανεξέταση και προσαρμογή της ασφαειακής πολιτικής.

ΚΕΦΑΛΑΙΟ 3: Αναλυτική παρουσίαση

ΑΝΑΛΥΤΙΚΗ ΠΑΡΟΥΣΙΑΚΗ ΤΩΝ ΠΑΝΕΠΙΣΤΗΜΙΑΚΩΝ ΤΜΗΜΑΤΩΝ ΣΤΟΝ ΤΟΜΕΑ ΤΙΣ ΑΣΦΑΛΕΙΑΣ

Στο κεφάλαιο αυτό θα παρουσιάσουμε διαφορετικά πανεπιστημιακά ιδρύματα, το τι διεξάγεται στο μάθημα της ασφάλειας των πληροφοριακών συστημάτων

Τα ιδρύματα Σχολών πληροφορικής που συλλέξαμε θα παρουσιαστούν παρακάτω αναλυτικά και με το διεξάγεται σε κάθε τμήμα, είναι τα εξής [19]

1.ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΣΧΟΛΗ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

1.1 ΕΙΣΑΓΩΓΗ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

1.2 : ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ

1.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα αυτό κατατάσσεται στα μαθήματα επιλογής του τμήματος και για μπορέσει κάποιος να το επιλέξει πρέπει πρώτα να έχει περάσει κάποια προ απαιτούμενα μαθήματα που είναι αλυσίδα του μαθήματος .Το συγκεκριμένο μάθημα διαθέτει και εργαστηριακό μέρος .Αρχικά, το μάθημα αυτό παρουσιάζει τις βασικές αρχές της κρυπτογραφίας ,και συνεχίζει με έναν αριθμό από σημαντικές εφαρμογές και πρακτικές τεχνικές και τέλος θέματα κρυπτογραφικής πολιτικής και διαχείρισης της ασφάλειας .Το μάθημα έχει σκοπό στο να γνωρίσουν οι φοιτητές τα προβλήματα ασφάλειας των ΠΣ , των δικτύων, τους μηχανισμούς και τεχνολογίες προστασίας και να κατανοήσουν τις παραμέτρους που καθιστούν αυτούς τους μηχανισμούς αποτελεσματικούς σε σύγχρονα συστήματα.

1.1.2 ΥΛΗ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγή: ιστορική αναδρομή, κλασσική κρυπτογραφία, σύγχρονες εφαρμογές
- Αρχιτεκτονική ασφάλειας: απειλές/επιθέσεις, μηχανισμοί/υπηρεσίες ασφάλειας, σχεδιασμός/πολιτικές ασφάλειας
- Συμμετρική κρυπτογραφία: κωδικοποιητές τμημάτων, αλγόριθμοι DES/3DES/AES, εφαρμογές/επιθέσεις
- Ασύμμετρη κρυπτογραφία: δομή κρυπτοσυστημάτων δημόσιου κλειδιού, ψηφιακές υπογραφές, διαχείριση κλειδιών, αλγόριθμοι **RSA/DSS/ECC**, εφαρμογές/επιθέσεις
- Αυθεντικοποίηση μηνυμάτων: ασφαλείς συναρτήσεις σύνυψης, αλγόριθμοι **MD5/SHA/HMAC**, εφαρμογές/επιθέσεις

- Κρυπτογραφικά πρωτόκολλα: αυθεντικοποίηση/διανομή κλειδιών, παραδείγματα(**passwords, challenge-response, needham-schroeder, kerberos**), αρχές σχεδιασμού/επιθέσεις
- Ασφάλεια στο Internet: πρωτόκολλα ασφάλειας επιπέδου Internet (**IPsec**) και επιπέδου μεταφοράς (**SSL, TLS, SSH**)
- Ασφάλεια εφαρμογών: ηλεκτρονικό ταχυδρομείο (**PGP, S/MIME**), ασφαλείς ηλεκτρονικές πληρωμές (**SET, micro-payments**)
- Υποδομή δημόσιων κλειδιών (**PKI**): ψηφιακά πιστοποιητικά, πάροχοι υπηρεσιών πιστοποίησης
- Λοιπές εφαρμογές: τραπεζικός τομέας (**ATM**), τηλεπικοινωνίες (**GSM, wireless**), ψηφιακά πνευματικά δικαιώματα (**DVD, Pay-TV**)
- Ασφάλεια λογισμικού και λειτουργικών συστημάτων: προγραμματιστικά λάθη, κρυπτογραφικές βιβλιοθήκες, **trusted computing base**
- Πρακτικά εργαλεία και τεχνικές: **Viruses, Worms, Bots, Spyware, Phishing**, διαχείριση ενημερωμένων εκδόσεων, εργαλεία επιτήρησης σταθμών εργασίας και δικτύων
- Διασφάλιση και αξιολόγηση ασφάλειας συστημάτων και προϊόντων: σκοπός, ζητήματα και μέθοδοι
- Ηλεκτρονικός πόλεμος: η πληροφορία σαν ανταγωνιστικό όπλο, κρίσιμες υποδομές, κυβερνοεπιθέσεις
- Κρυπτογραφική πολιτική: νομοθεσία, ιδιωτικότητα, ανωνυμία, προστασία δεδομένων, πνευματική ιδιοκτησία
- Οικονομικά της ασφάλειας: τεχνολογικά/οικονομικά κίνητρα για την ανάπτυξη ασφαλών προϊόντων Μαθησιακοί στόχοι: Οι φοιτητές μετά την επιτυχή ολοκλήρωση του μαθήματος :
 - Θα κατέχουν τις βασικές έννοιες της ασφάλειας πληροφοριών και δικτύων
 - Θα έχουν εξοικειωθεί με βασικά εργαλεία κρυπτογράφησης και αποκρυπτογράφησης
 - Θα έχουν μάθει τις βασικές αρχές της θεωρίας κρυπτογραφίας και προστασίας δικτύων
 - Θα έχουν μάθει τις βασικές αρχές επιθέσεων στο διαδίκτυο και εντοπισμού κακόβουλου λογισμικού, και
 - Θα είναι σε θέση να υλοποιήσουν νέα εργαλεία ασφάλειας και προστασίας στο διαδίκτυο

1.1.3 ΜΑΘΗΣΙΑΚΟΙ ΣΤΟΧΟΙ

Οι φοιτητές μετά την επιτυχή ολοκλήρωση του μαθήματος ▪ θα κατέχουν τις βασικές έννοιες της ασφάλειας πληροφοριών και δικτύων

- θα έχουν εξοικειωθεί με βασικά εργαλεία κρυπτογράφησης και αποκρυπτογράφησης
- θα έχουν μάθει τις βασικές αρχές της θεωρίας κρυπτογραφίας και προστασίας δικτύων
- θα έχουν μάθει τις βασικές αρχές επιθέσεων στο διαδίκτυο και εντοπισμού κακόβουλου λογισμικού, και
- θα είναι σε θέση να υλοποιήσουν νέα εργαλεία ασφάλειας και προστασίας στο διαδίκτυο[4]

1.2.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα είναι επιλογής και έχει προ απαιτούμενά συγκεκριμένα μαθήματα για το επιλέξει κάποιος φοιτητής κατά την διάρκεια των σποδών του. Αρχικά, στο μάθημα θα αναπτυχθούν θέματα όπως ο σωστός χειρισμός των πειστηρίων στον τόπο του εγκλήματος, τρόποι ανάκτησης πειστηρίων και διατήρησης της ακεραιότητας αυτών κατά την διάρκεια της έρευνας καθώς και ενδεικνυόμενες προσεγγίσεις σχετικά με τη συγγραφή των συμπερασμάτων της έρευνας και πειστικής παρουσίασης αυτών σε ένα δικαστήριο. Επίσης, θα επιδειχθεί η χρήση σχετικών εργαλείων, τόσο ανοικτού κώδικα όσο και εμπορικών προγραμμάτων, και θα δοθεί έμφαση στην επαλήθευση των αποτελεσμάτων που προκύπτουν από την χρήση αυτών. Επίσης, κατά τη διάρκεια του μαθήματος θα συζητηθούν τεχνικές που σε ένα βαθμό παρακάμπτουν μέτρα ασφάλειας και ανακτούν δεδομένα σε πιο απαιτητικές περιπτώσεις με απώτερο στόχο την ορθή ανάλυση των ψηφιακών πειστηρίων που συγκεντρώνονται σε μία εγκληματολογική έρευνα. Τέλος, οι φοιτητές θα εξοικειωθούν στη χρήση τεχνικών εργαλείων, προκειμένου να αναλύουν τα πειστήρια με τον βέλτιστο τρόπο και συνολικά να ολοκληρώνουν την έρευνα με αποδοτικό και ποιοτικό τρόπο. Ο σκοπός του μαθήματος είναι παρουσίαση μεθόδων, σύγχρονων βέλτιστων πρακτικών και προτύπων που συνίσταται να ακολουθούνται κατά την διάρκεια μίας εγκληματολογικής έρευνας που συμπεριλαμβάνει ψηφιακές συσκευές και δεδομένα.

1.2.2 ΜΑΘΗΣΙΑΚΟΙ ΣΤΟΧΟΙ

- Περιγραφή των βασικών αρχών της ψηφιακής εγκληματολογίας και των ιδιαίτερων προκλήσεων σχετικά με κινητές συσκευές
- Περιγραφή και σύγκριση διαφόρων τεχνικών σχετικά με την ανάκτηση και ανάλυση ψηφιακών δεδομένων σε μία εγκληματολογική έρευνα.
- Περιγραφή και σύγκριση των λειτουργικών συστημάτων **Android** και **IOS** και παρουσίαση μεθόδων για την κατά το δυνατό παράκαμψη των μέτρων ασφάλειας που προσφέρουν.
- Δυνατότητα αξιοποίησης εργαλείων ανοικτού κώδικα καθώς και εμπορικών προγραμμάτων.
- Δυνατότητα αξιολόγησης των ψηφιακών πειστηρίων και σωστός χειρισμός αυτών για την διατήρηση της αποδεικτικής τους αξίας.
- Διαχείριση του τόπου του εγκλήματος με βάση τα στοιχεία της υπόθεσης και την αξιοποίηση βέλτιστων πρακτικών, προτύπων και του εφαρμοστέου νομικού καθεστώτος.
- Καταγραφή των στοιχείων της έρευνας και παρουσίαση αυτών με τρόπο που να είναι αποδεκτός στις δικαστικές αρχές[4]

2.ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ - ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

2.1 ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

2.2 ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΔΙΚΤΥΑΚΩΝ ΕΦΑΡΜΟΓΩΝ

2.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα αυτό είναι υποχρεωτικό κατά την διάρκεια σπουδών και από ότι παρατηρείτε δεν χρειάζεται προ απαιτούμενά μαθήματα για την παρακολούθηση του.

- Εισαγωγή (Βασικές Έννοιες, Παραβάσεις Ασφάλειας, Ευπάθειες, Απειλές, Μέτρα Προστασίας, Απαιτήσεις Ασφάλειας ΠΣ, Προστασία των Προσωπικών Δεδομένων)
- Ασφάλεια Προσωπικών Υπολογιστών - Κακόβουλα Προγράμματα (Ιοί, Σκουλήκια, Δούρειοι Ίπποι) Αναγνώριση και Αυθεντικοποίηση (Τεχνικές, μέσα, πρότυπα, διαδικασίες και ζητήματα, Υλοποιήσεις σε γνωστά λειτουργικά συστήματα)
- Έλεγχος Προσπέλασης (Κατά διάκριση, Κατά απαίτηση, Βασισμένος σε ρόλους, Επεκτάσεις και Υλοποιήσεις σε γνωστά λειτουργικά συστήματα)
- Πολιτικές και Μοντέλα Ασφάλειας Π.Σ. (**Clark-Wilson, Harrison-Ruzzo-Ullman, Graham-Denning, Chinese Wall, Bell-La Padula, Biba**, Πολιτικές Ασφάλειας Υψηλού Επιπέδου).
- Ανάλυση και Αποτίμηση Επικινδυνότητας (Θεωρητικές προσεγγίσεις, Παραδείγματα εφαρμογής, Εργαλεία **Cramm** και **Cobra**)
- Αξιολόγηση Ασφάλειας Υπολογιστικών Συστημάτων (Κριτήρια **TCSEC**, Κριτήρια **ITSEC**, **Federal criteria (FF)**, **Common Criteria (CC)**)
- Ασφάλεια Συστημάτων Βάσεων Δεδομένων (Συστατικά και χώροι ορισμού ασφάλειας, Υλοποιήσεις στο ΣΔΒΔ **ORACLE**)
- Ψηφιακή εγκληματολογία απόκριση περιστατικών ασφάλειας (**Digital Forensics * Incident Response**) Κυβερνοασφάλεια - Προσωπικά Δεδομένα

2.2.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα κατά το πρόγραμμα σπουδών είναι επιλογής και όπως καταγράφετε δεν χρειάζεται προ-απαιτούμενά μαθήματα για την παρακολούθηση του.

- Βασικές Έννοιες (Προβλήματα ασφάλειας δικτύων και διαδικτύου,
- Τύποι επιθέσεων και μέτρων προστασίας, Σύγκριση τεχνολογιών ασφάλειας)
- Εισαγωγή στην Κρυπτογραφία (Ορολογία, Τύποι κρυπτογραφικών συστημάτων και χαρακτηριστικά των συστατικών τους, Γεννήτριες κλειδαριών)
- Κλασσικοί Κρυπτογραφικοί Αλγόριθμοι και Κρυπτανάλυση (**Caesar, Vigenere, One Time Pad / Vernam, ROT13**, Αλγόριθμοι Μετατόπισης, Αλγόριθμοι Αντικατάστασης, Εφαρμογές με το εργαλείο **CRYPTOOL**)

- Σύγχρονοι Συμμετρικοί Κρυπτογραφικοί Αλγόριθμοι και Κρυπτανάλυση (**DES, 3-DES, AES, IDEA, RC2, RC4**, κλπ.,
- Τρόποι λειτουργίας (**ECB, CBC, OFB, CFB**), Εφαρμογές με το εργαλείο **CRYPTOOL**)
- Σύγχρονοι Ασύμμετροι Κρυπτογραφικοί Αλγόριθμοι και Κρυπτανάλυση (**Diffie-Hellman, DSA, RSA, ECC**,
- Εφαρμογές με το εργαλείο **CRYPTOOL**) Μηχανισμοί Ακεραιότητας (**CBC-MAC, HMAC, OWHF, CRHF, MD5, SHA, DSS**, κλπ.,
- Εφαρμογές με το εργαλείο **CRYPTOOL**)
- Εφαρμογές της Κρυπτογραφίας (**message digests, digital signatures, digital certificates**, κλπ)
- Υποδομές Πιστοποίησης (Συστατικά και Ιδιότητες Υποδομών Δημοσίου Κλειδιού – **PKI**)
- Προστασία Ψηφιακών Επικοινωνιών (**S/MIME, PGP, SSL/TLS, IPsec**, κλπ)
- Ασφάλεια Ενσύρματων Δικτύων και Εφαρμογών Διαδικτύου (Ζητήματα, Κρίσιμες αδυναμίες, Είδη επιθέσεων, Μελέτες περιπτώσεων)
- Προστασία με **Firewalls** και **IDS** (Είδη μηχανισμών, Αρχιτεκτονικές, Μελέτες περιπτώσεων) [5]

3. ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

3.1 ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

3.2 ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

3.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα στο πρόγραμμα σπουδών είναι επιλογής και για την επιλογή του απαιτεί να υπάρχει επιτυχής εξέταση σε προ απαιτούμενα μαθήματα είτε στο μάθημα «Λειτουργικά Συστήματα» είτε στο μάθημα «Προγραμματισμός Υπολογιστών με **JAVA**».

- Εννοιολογική Θεμελίωση: Βασικές έννοιες και ορισμοί.
- Σχέσεις και διαφοροποιήσεις. Ανάλυση και απεικόνιση μέσω διαγραμμάτων **E-R**.
- Αποτίμηση Επικινδυνότητας: Στόχοι, δυνατότητες και περιορισμοί τεχνικών ανάλυσης και διαχείρισης επικινδυνότητας. Παραδείγματα τεχνικών (**CRAMM, OC-TAVE** κλπ.).
- Έλεγχος Προσπέλασης: Ταυτοποίηση, αυθεντικοποίηση, εξουσιοδότηση, χρήση μεθόδων **CAPTCHA**, αγνωστικά και πιθανοτικά πρωτόκολλα, βιομετρικές τεχνολογίες.
- Εισαγωγή στην Κρυπτολογία: Εννοιολογική θεμελίωση.

- Συμμετρική και Ασύμμετρη Κρυπτογραφία. Υποδομές Δημόσιου Κλειδιού (**PKI**).
- Ψηφιακές υπογραφές/πιστοποιητικά.
- Κρυπτανάλυση. Αξιοποίηση Κρυπτολογίας. Ιομορφικό Λογισμικό: Οριοθέτηση και ταξινόμηση. Δούρειοι ίπποι, αναπαραγωγοί (**worms**), προγράμματα ιού. Αλγοριθμική προσέγγιση.
- Θεμελιώσεις: Cohen (**Turing Machines**), **Adleman** (αριθμητική **Goedel**), Kerphart (κατευθυνόμενοι γράφοι).
- Πολιτικές, μέθοδοι και τεχνικές προληπτικής και κατα-σταλτικής αντιμετώπισης. Ασφάλεια στο Διαδίκτυο, **Hackers** και **Hacking**: Θεωρία τεσσάρων ασυνεχειών. Μορφότυποι **hackers**. **Ethics of Security**. **Hacking** και **Hactivism**. Ασφάλεια ασύρματων τοπικών δικτύων (**WLAN**).
- Λογισμικό αξιολόγησης και ελέγχου ασφάλειας (**Openvas|Nessus, Metasploit, Nmap, Aircracking** κλπ.).
- Προστασία Προσωπικών Δεδομένων: Ιδιωτικότητα (**privacy**) και προστασία προσωπικών δεδομένων. Θεσμικό πλαίσιο. Οπτική, ρόλος και ευθύνη των Πληροφορικών.
- Ασφάλεια στο Απантаχού Υπολογίζουν: Ασφάλεια στο **Cloud Computing**. **Internet of Things**. Στρατηγικές ασφάλειας και ιδιωτικότητας στην Κοινωνία της Πληροφορίας και της Γνώσης. Εξειδικευμένα πεδία εφαρμογής ασφάλειας και προάσπισης ιδιωτικότητας (**OSN, VoIP**, κρίσιμες υποδομές κλπ.).

3.1.2 ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μετά την επιτυχή ολοκλήρωση του μαθήματος, οι φοιτητές θα είναι σε θέση:

- Να κατανοούν σε βάθος και να μπορούν να χρησιμοποιήσουν την ορολογία της Ασφάλειας Πληροφοριακών Συστημάτων.
- Να συνδράμουν στη σχεδίαση και εφαρμογή σχεδίων και πολιτικών ασφάλειας πληροφοριακών συστημάτων.
- Να αποτιμήσουν την επικινδυνότητα ενός πληροφοριακού συστήματος, με χρήση κατάλληλων εργαλείων.
- Να σχεδιάσουν, να εφαρμόσουν και να αποτιμήσουν ένα σύστημα ελέγχου προσπέλασης σε ένα σύστημα.
- Να αξιολογήσουν και να επιλέξουν το κατάλληλο κρυπτοσύστημα για την προστασία ενός συστήματος.
- Να προστατεύσουν ένα πληροφοριακό σύστημα αξιοποιώντας τεχνικές και μεθόδους Κρυπτολογίας.
- Να αντιμετωπίσουν μια προσβολή από ιομορφικό λογισμικό (ιός, αναπαραγωγός, δούρειος ίππος κλπ.).

- Να ελέγχουν την ασφάλεια (**penetration testing**) ενός πληροφοριακού συστήματος ή μιας εφαρμογής.
- Να εκτιμήσουν τη σημασία του κοινωνικο-πολιτικού συμφραζόμενου (**context**) στην ανάγκη προστασίας ενός πληροφοριακού συστήματος και να κατανοήσουν τους εμφανιζόμενους μορφότευπους (**hacker, cracker** κλπ.).
- Να αποτιμήσουν, να αναδείξουν και να υποστηρίξουν τη σημασία τήρησης της ιδιωτικότητας (**privacy**).
- Να κατανοήσουν και να εφαρμόσουν την κείμενη νομοθεσία για την προστασία προσωπικών δεδομένων.

3.2.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα είναι επιλογής και για την εγγραφή του χρειάζεται προ απαιτούμενά μαθήματα με επιτυχή εξέταση στα παρακάτω συγκεκριμένα μαθήματα είτε στο μάθημα «Δίκτυα Επικοινωνιών» είτε στο μάθημα «Δίκτυα Υπολογιστών».

- Εισαγωγή σε κρυπτογραφικές τεχνικές (συμμετρικές, δημοσίου κλειδιού) και τεχνικές σύνοψης, ατέλειες τεχνικών.
- Αυθεντικοποίηση στο διαδίκτυο (μοντέλα **Needham-Schroeder, Kerberos, Lamport S/Keys, OTPs, MAC/EAP**), ευπάθειες και απειλές στο τοπικό δίκτυο και στο διαδίκτυο (υποκλοπή, πλαστογράφηση, αναπαραγωγή, επίθεση ενδιάμεσου, πειρατεία).
- Τεχνικές άμυνας, αντιμέτρα ασφάλειας και διαθεσιμότητα (αναχώματα ασφαλείας, ανίχνευση/αποτροπή εισβολών).
- Ασφαλή πρωτόκολλα και υπηρεσίες σε δίκτυα **IP (VPNs, IPSec/IKE, ασφάλεια στο IPv6, ασφαλής δρομολόγηση, ασφαλής διαχείριση δικτύων, NAT/PAT, DNS security, SSL/TLS/SSH, PGP/S-MIME)**.
- Υπηρεσίες πιστοποίησης και πάροχοι. Ιδιωτικότητα, ακεραιότητα και αυθεντικοποίηση σε ασύρματα δίκτυα και δίκτυα κινητής τηλεφωνίας.
- Ασφάλεια εφαρμογών διαδικτύου (**Cookies, HTTPs, Digest Authentication**). Κακόβουλοι και Ιομορφικό Λογισμικό.
- Μελέτες ειδικών περιπτώσεων, εργαστηριακές ασκήσεις και πρακτικές εφαρμογές.

ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μετά την επιτυχή ολοκλήρωση του μαθήματος, οι φοιτητές θα είναι σε θέση:

- Να αντιλαμβάνονται θέματα ασφάλειας δικτύων και υπολογιστών όπως αυτά πραγματεύονται και εξελίσσονται σε διεθνείς οργανισμούς, όπως το **ISO/OSI, ITU, IETF** και το **IEEE, NIST, ETSI**.
- Να κάνουν την αντιστοίχιση αναγκών και μέτρων ασφαλείας με μηχανισμούς ασφαλείας δικτύων/υπολογιστών και κρυπτογραφικές τεχνικές.
- Να κατανοούν τις αδυναμίες και τις επιθέσεις σε υπολογιστές και σε όλα τα επίπεδα δικτύωσης, καθώς και των αντιμέτρων που έχουν προταθεί και εφαρμόζονται ευρέως.

- Να γνωρίζουν τις ανάγκες προστασίας της ιδιωτικότητας στον ιστό και να έχουν διδαχθεί σχετικές τεχνικές ενίσχυσής της.
- Να κατανοούν τη λειτουργία και τη σκοπιμότητα των Internet πρωτοκόλλων ασφάλειας, αλλά κυρίως τις αδυναμίες τους και τους τρόπους προστασίας από αυτές.
- Να γνωρίζουν σύγχρονα θέματα ασφάλειας και προστασίας, όπως αρχιτεκτονικές ταυτοποίησης και διαχείρισης εμπιστοσύνης.
- Να αναγνωρίζουν σύγχρονες απειλές ασφάλειας και τρόπους αντιμετώπισής τους.[9]

4. ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

4.1 ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

4.1.1 ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

- Προγραμματισμός ταυτοχρονισμού και Ασφάλεια Λογισμικού
- Αξιοπιστία και Ασφάλεια Λογισμικού.

ΜΑΘΗΣΙΑΚΟΙ ΣΤΟΧΟΙ

Οι φοιτητές αναμένεται ότι στα πλαίσια του μαθήματος θα:

- μάθουν να αναπτύσσουν προγράμματα ταυτοχρονισμού
- μπορούν να επαληθεύσουν προγράμματα ταυτοχρονισμού ως προς την ορθότητά τους
- μπορούν να διατυπώνουν αλγόριθμους επίλυσης προβλημάτων σε κατακευκτωμένα συστήματα με βάση θεμελιώδη κριτήρια ορθότητας
- εξοικειωθούν με τον προγραμματισμό μηχανισμών ασφάλειας λογισμικού
- εξοικειωθούν με προβλήματα ασφάλειας εφαρμογών λογισμικού[6]

5. ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

5.1 ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

5.2 ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

5.3 ΑΣΦΑΛΕΙΑ ΛΟΓΙΣΜΙΚΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ

5.4 ΔΙΟΙΚΗΣΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

5.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα το συγκεκριμένο που αναφέρουμε είναι μάθημα κορμού, δηλαδή, είναι βασικό μάθημα για την διεξαγωγή συνέχεια κάποιων άλλων μαθημάτων στο πρόγραμμα σπουδών.

- Εισαγωγή στην Ασφάλεια: Βασικοί ορισμοί, Μοντέλο Απειλών, Υπηρεσίες Ασφάλειας.
- Εισαγωγή στις έννοιες: Απειλή, Ευπάθεια, Κίνδυνος. Ασφάλεια Συστήματος – Έλεγχος Λογικής
- Πρόσβασης – Τοπική και Απομακρυσμένη Αυθεντικοποίηση Οντότητας: Κωδικοί **Passwords**,
- Απομακρυσμένη Αυθεντικοποίηση με κρυπτογραφικές τεχνικές, Κωδικοί μιας χρήσης,
- Ταυτοποίηση με Μηδενική Γνώση. Έλεγχος Λογικής Πρόσβασης – Εξουσιοδότηση: Πολιτικές και μοντέλα εξουσιοδότησης (**MAC, DAC, RBAC**). Ασφάλεια Λειτουργικού Συστήματος.
- Κακόβουλο λογισμικό: Μοντέλο Απειλών, μηχανισμοί αντιμετώπισης, ερευνητικά θέματα.
- Αυθεντικοποιημένη εδραίωση κλειδιού και Εφαρμογές: Συστήματα Διανομής κλειδιού,
- Συστήματα Μεταφοράς Κλειδιού, Συστήματα Συμφωνίας Κλειδιού. Ασφάλεια Δικτύων:
- Μοντέλο απειλών στο Επίπεδο **TCP/IP**, ασφάλεια υπηρεσιών Διαδικτύου, ασφάλεια στο Web.
- Δικτυακά Συστήματα **Firewalls**

➤ ΣΚΟΠΟΣ ΤΟΥ ΜΑΘΗΜΑΤΟΣ

- Η εισαγωγή στις βασικές έννοιες της ασφάλειας συστημάτων και επικοινωνιών.
- Η επισημάνση των αδυναμιών των συμβατικών τεχνικών ταυτοποίησης με κωδικούς πρόσβασης, καθώς και η διόρθωση ορισμένων από αυτές τις αδυναμίες με κρυπτογραφικό τρόπο. Επίσης, η κατανόηση των κρυπτογραφικών τεχνικών ταυτοποίησης απομακρυσμένης οντότητας για τον έλεγχο λογικής πρόσβασης στην ασφάλεια υπολογιστικών συστημάτων και δικτύων.
- Η κατανόηση και εφαρμογή των μοντέλων εξουσιοδότησης στην ασφάλεια συστημάτων.
- Η κατανόηση του μοντέλου ασφάλειας στα πλέον δημοφιλή Λ.Σ.
- Η ανάλυση και αντιμετώπιση των διάφορων τύπων κακόβουλο λογισμικού. Με την επιτυχή ολοκλήρωση του μαθήματος ο/η φοιτητής/φοιτήτρια θα είναι σε θέση να:
- Αναλύει έναν πληροφοριακό κίνδυνο στα συστατικά του στοιχεία,

- Διακρίνει τη διαφορά μεταξύ Αυθεντικοποίησης οντότητας και Αυθεντικοποίησης μηνύματος,

- Περιγράφει και να εφαρμόζει τις τεχνικές που χρησιμοποιούν οι κρυπτογραφικοί μηχανισμοί Αυθεντικοποίησης απομακρυσμένης οντότητας,

Βρίσκει τα αδύναμα σημεία ενός πρωτοκόλλου απομακρυσμένης Αυθεντικοποίησης, καθώς και να εξαπολύει παθητικές ή/και ενεργητικές επιθέσεις εναντίον του,

- Διορθώνει, κάνοντας χρήση των κατάλληλων κρυπτογραφικών μηχανισμών, τις ευπάθειες ενός κρυπτογραφικού πρωτοκόλλου απομακρυσμένης Αυθεντικοποίησης οντότητας,

- Καθορίζει τις επιτρεπόμενες προσβάσεις σε ένα σύστημα, βάσει διαφόρων μοντέλων εξουσιοδότησης

- Αναγνωρίζει και να διορθώνει τις απειλές/ευπάθειες στην ασφάλεια ενός συστήματος,

- Αναγνωρίζει και να αντιμετωπίζει ένα κακόβουλο λογισμικό από τη συμπεριφορά του στο σύστημα που προσέβαλε.

5.2.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα το οποίο αν αναφέρεται είναι επιλογής στο πρόγραμμα σπουδών

- Βασικές αρχές κρυπτογραφίας. Εξασφάλιση εμπιστευτικότητας, ακεραιότητας δεδομένων και αυθεντικοποίηση.
- Επιθέσεις αντανάκλασης και ενδιαμέσου.
- Συστήματα συμφωνίας και διανομής κλειδιού. Το πρωτόκολλο **Kerberos**. Ασφάλεια Ασύρματων δικτύων και πρωτόκολλα ασφάλειας **WPA/WPA2**.
- Ασφάλεια σε κινητά δίκτυα **GSM/UMTS/LTE**. Μοντέλο απειλών στο Επίπεδο **TCP/IP**. Ανάλυση του πρωτοκόλλου **TLS/SSL**.
- Ανάλυση του μηχανισμού **Pretty Good Privacy**.
- Ανάλυση, εφαρμογή και αξιολόγηση των αναχωμάτων ασφάλειας (**Firewalls**) και εικονικών δικτύων (**Virtual Private Networks**).
- Επιθέσεις παρεισφρήσεων (**intrusions**) και μηχανισμοί ανίχνευση εισβολών (**intrusion detection systems**) σε δικτυακά συστήματα, Επιθέσεις άρνησης παροχής υπηρεσιών στο Διαδίκτυο και τρόποι αντιμετώπισης τους.
- Επιθέσεις στο πρωτόκολλο Domain Name System (**DNS**) και **Address Resolution Protocol (ARP)**. Εισαγωγή στο κακόβουλο λογισμικό διαδικτύου και **botnets**.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ :

Με την επιτυχή ολοκλήρωση του μαθήματος ο/η φοιτητής/φοιτήτρια θα είναι σε θέση να:

- Καθορίσει τις απαιτήσεις ασφάλειας ενός δικτυακού συστήματος.

- Έχει κατανόηση των κενών ασφάλειας και των απειλών που διατρέχουν τα δίκτυα υπολογιστών και οι δικτυακές/διαδικτυακές εφαρμογές.
- Σχεδιάσει μηχανισμούς και πρωτόκολλα ασφάλειας που ικανοποιούν καλά προσδιορισμένες απαιτήσεις και προστατεύουν από συγκεκριμένες απειλές.
- Εφαρμόσει τις γνώσεις του για να προστατεύσει τις συσκευές και την διακινούμενη δικτυακά πληροφορία από κακόβουλες ενέργειες
- Αναγνωρίσει και να συνεισφέρει στις τρέχουσες εξελίξεις και προκλήσεις στο χώρο.

5.3.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

- Επιθέσεις λογισμικού με τεχνικές υπερχείλισης μνήμης.
- Ανάλυση πηγαίου κώδικα. Τεχνικές **Fuzzing** για αυτοματοποιημένη εύρεση λογικών σφαλμάτων και ευπαθειών λογισμικού.
- Σύγχρονες τεχνικές εκμετάλλευσης ευπαθειών λογισμικού. Ανέλιξη δικαιωμάτων σε συστήματα **Linux** και **Windows**.
- Εκτίμηση αδυναμιών και έλεγχος ασφάλειας πληροφοριακών συστημάτων. Εισαγωγή σε τεχνολογίες **Web**, όπως **PHP, HTML, SQL, JavaScript**.
- Επιθέσεις **Cross Site Scripting attacks (XSS)** και **Cross Site Request Forgery (CSRF)**. Επιθέσεις **SQL injection** και **Local file inclusion (LFI)**.
- Σφάλματα στην αυθεντικοποίηση, διαχείριση συνόδου, μηχανισμούς ελέγχου πρόσβασης και σε κρυπτογραφικές λύσεις. Έλεγχος ασφάλειας εφαρμογών Διαδικτύου.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ :

Με την επιτυχή ολοκλήρωση του μαθήματος ο/η φοιτητής/φοιτήτρια θα είναι σε θέση να:

- Να αναλύσουν και να αξιολογήσουν πηγαίο κώδικα για εύρεση καινούργιων αδυναμιών καθώς και εκμετάλλευσή τους για εκδήλωση επιθέσεων.
- Να εφαρμόσουν μεθοδολογίες και τεχνικές **penetration testing** στη μελέτη ασφάλειας ενός πληροφοριακού συστήματος.
- Να χρησιμοποιήσουν μια σειρά από εργαλεία ανοιχτού κώδικα τα οποία χρησιμοποιούνται ευρέως στο χώρο της ασφάλειας πληροφοριακών συστημάτων.
- Να πραγματοποιούν έλεγχο ασφάλειας σε εφαρμογές Διαδικτύου.
- Να γνωρίζουν τις βασικότερες επιθέσεις σε εφαρμογές Διαδικτύου.
- Να γνωρίζουν τις τρέχουσες τάσεις της έρευνας και να εκτιμήσουν την επίδραση που αυτές μπορεί να έχουν στο χώρο τα επόμενα χρόνια.

5.4.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα κατά το πρόγραμμα σποδών είναι επιλογής.

- Επιθέσεις λογισμικού με τεχνικές υπερχείλισης μνήμης.
- Ανάλυση πηγαίου κώδικα. Τεχνικές **Fuzzing** για αυτοματοποιημένη εύρεση λογικών σφαλμάτων και ευπαθειών λογισμικού.
- Σύγχρονες τεχνικές εκμετάλλευσης ευπαθειών λογισμικού. Ανέλιξη δικαιωμάτων σε συστήματα **Linux** και **Windows**.
- Εκτίμηση αδυναμιών και έλεγχος ασφάλειας πληροφοριακών συστημάτων. Εισαγωγή σε τεχνολογίες **Web**, όπως **PHP**, **HTML**, **SQL**, **JavaScript**.
- Επιθέσεις **Cross Site Scripting attacks (XSS)** και **Cross Site Request Forgery (CSRF)**.
- Επιθέσεις **SQL injection** και **Local file inclusion (LFI)**. Σφάλματα στην αυθεντικοποίηση, διαχείριση συνόδου, μηχανισμούς ελέγχου πρόσβασης και σε κρυπτογραφικές λύσεις.
- Έλεγχος ασφάλειας εφαρμογών Διαδικτύου

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Με την επιτυχή ολοκλήρωση του μαθήματος ο/η φοιτητής/φοιτήτρια θα είναι σε θέση να:

- Να αναλύσουν και να αξιολογήσουν πηγαίο κώδικα για εύρεση καινούργιων αδυναμιών καθώς και εκμετάλλευσή τους για εκδήλωση επιθέσεων.

Να εφαρμόσουν μεθοδολογίες και τεχνικές **penetration testing** στη μελέτη ασφάλειας ενός πληροφοριακού συστήματος.

- Να χρησιμοποιήσουν μια σειρά από εργαλεία ανοιχτού κώδικα τα οποία χρησιμοποιούνται ευρέως στο χώρο της ασφάλειας πληροφοριακών συστημάτων.
- Να πραγματοποιούν έλεγχο ασφάλειας σε εφαρμογές Διαδικτύου.
- Να γνωρίζουν τις βασικότερες επιθέσεις σε εφαρμογές Διαδικτύου.
- Να γνωρίζουν τις τρέχουσες τάσεις της έρευνας και να εκτιμήσουν την επίδραση που αυτές μπορεί να έχουν στο χώρο τα επόμενα χρόνια.

5.4.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

- Εννοιολογικό πλαίσιο διοίκησης ασφάλειας. Σχεδιασμός ασφάλειας: προσεγγίσεις και ανάλυση επικινδυνότητας.
- Μέθοδοι και εργαλεία λογισμικού για την ανάλυση επικινδυνότητας (**CRAMM**, **OCTAVE**, **SBA analysis**).
- Πρότυπα διακυβέρνησης ασφάλειας. Πλαίσια, οδηγίες και πιστοποιήσεις για την διοίκηση ασφάλειας πληροφοριακών συστημάτων (**ISO 27001**, **ISO 27002**, **NIST SP 800-30**, κ.ά.) Επιθεώρηση ασφάλειας πληροφοριακών συστημάτων.

- Πολιτικές ασφάλειας. Σκοπός, δομή και περιεχόμενα οργανωσιακών πολιτικών ασφάλειας. Παραδείγματα γενικευμένων και εξειδικευμένων πολιτικών ασφάλειας. Διαχείριση Περιστατικών Ασφάλειας.
- Σχεδιασμός για τη διαχείριση περιστατικών ασφάλειας, βήματα αντιμετώπισης περιστατικών ασφάλειας. Επιχειρησιακή συνέχεια και σχέδιο ανάκαμψης από καταστροφή. Ενημερότητα ασφάλειας.
- Ο Γενικός Κανονισμός για την Προστασία Δεδομένων. Ανάλυση αντικτύπου για την προστασία δεδομένων.
- Μέθοδοι και εργαλεία λογισμικού για την υλοποίηση ανάλυσης αντικτύπου παραβίασης προσωπικών δεδομένων. Μέτρηση ασφάλειας πληροφοριών.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Το μάθημα αποσκοπεί στην απόκτηση γνώσεων και την κατανόηση θεμάτων σχετικών με τη διοίκηση ασφάλειας πληροφοριών σε οργανωσιακά περιβάλλοντα. Η ύλη του μαθήματος και η διδασκαλία έχουν σχεδιαστεί ώστε να στοχεύουν αρχικά στην κατανόηση από τους φοιτητές ενός εννοιολογικού πλαισίου για το επιστημονικό πεδίο της διοίκησης ασφάλειας πληροφοριακών συστημάτων. Στο πλαίσιο του μαθήματος αναλύονται μέθοδοι ανάλυσης και διαχείρισης επικινδυνότητας ασφάλειας πληροφοριών, με επίδειξη εργαλείων λογισμικού όπου αυτά απαιτούνται και ανάλυση μελετών περίπτωσης, με στόχο τη γνώση και απόκτηση δεξιοτήτων εφαρμογής τέτοιων μεθόδων στην πράξη. Επιπλέον, αναλύονται τεχνικά πρότυπα διοίκησης ασφάλειας πληροφοριών και σχετικές πιστοποιήσεις. Ενθαρρύνεται η αναγνώριση της σημασίας της διοίκησης ασφάλειας πληροφοριακών συστημάτων σε σύγχρονους οργανισμούς και οι σχετικοί επαγγελματικοί ρόλοι που συναντώνται στη σημερινή αγορά εργασίας.

Με την επιτυχή ολοκλήρωση του μαθήματος ο/η φοιτητής/φοιτήτρια θα είναι σε θέση να:

- Έχει κατανοήσει τις κύριες έννοιες της διοίκησης ασφάλειας πληροφοριών (π.χ. επικινδυνότητα, απειλή, ευπάθεια).

Έχει τη γνώση και τις δεξιότητες να εφαρμόσει μεθόδους και εργαλεία για την ανάλυση επικινδυνότητας ασφάλειας πληροφοριακών συστημάτων,

- Είναι σε θέση να αναλύσει ένα πληροφοριακό σύστημα και το αντίστοιχο οργανωσιακό περιβάλλον, αναφορικά με τις απαιτήσεις ασφάλειας πληροφοριών του, να προτεραιοποιήσει τις απαιτήσεις αυτές, και να τεκμηριώσει μέτρα προστασίας,

- Έχει τη γνώση και τις δεξιότητες για την ανάπτυξη πολιτικών ασφάλειας για τη διαχείριση επικινδυνότητας,

- Έχει την ικανότητα να συγκεντρώσει και να αξιολογήσει στοιχεία για την αξιοποίηση των διαθέσιμων τεχνικών προτύπων ασφάλειας πληροφοριών,

- Γνωρίζει το ευρύτερο πεδίο της διοίκησης ασφάλειας πληροφοριακών συστημάτων, αλλά και των επιμέρους ερευνητικών και πρακτικών προκλήσεων και της μεταξὺ τους σύνδεσης [7]

6. ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

6.1 ΔΙΟΙΚΗΣΗ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ

6.2 ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

6.3 ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

6.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα κατά το πρόγραμμα σποδών είναι επιλογής

- Συνήθη κενά ασφαλείας πληροφοριακών συστημάτων και εφαρμογών
- Μέθοδοι και εργαλεία εντοπισμού κενών ασφαλείας πληροφοριακών συστημάτων και εφαρμογών
- **Exploitation & persistence**
- Ψηφιακά πειστήρια
- Μεθοδολογίες Ανάλυσης Πληροφοριακού Κινδύνου (**information risk analysis**)
- Σχέδια, Πολιτικές και Διαδικασίες Ασφάλειας
- Κανονιστικό Πλαίσιο και Πρότυπα Ασφάλειας.
- Σχέδια Συνέχειας Λειτουργίας και Ανάκαμψης Συστημάτων.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μετά την επιτυχή ολοκλήρωση του μαθήματος, οι φοιτητές θα είναι σε θέση:

- Να γνωρίζουν τις μεθόδους και τα εργαλεία εντοπισμού κενών ασφαλείας
- Να διακρίνουν πιθανά κενά ασφαλείας σε ένα πληροφοριακό σύστημα
- Να κατανοούν τα συνήθη κενά ασφαλείας πληροφοριακών συστημάτων και εφαρμογών
- Να εντοπίζουν πιθανές επιθέσεις μετά από ανάλυση των **log files**
- Να διερευνούν και να αξιολογούν κενά ασφαλείας μιας διαδικασίας ενός οργανισμού
- Να αναγνωρίζουν και να διαχειρίζονται τις μεθοδολογίες ανάλυσης πληροφοριακών κινδύνων
- Να σχεδιάζουν και να εφαρμόζουν μια πολιτική ασφαλείας σε έναν οργανισμό

Κεντρικός στόχος του μαθήματος

είναι οι φοιτητές να μπορούν να αξιολογήσουν την ασφάλεια που προσφέρει ένα πληροφοριακό σύστημα καθώς και την ποιότητα της ασφάλειας που παρέχεται από την εφαρμογή των διαδικασιών ενός οργανισμού.

6.2.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα κατά το πρόγραμμα σπουδών είναι υποχρεωτικό κατά την διάρκεια των σπουδών.

ασφάλεια της πληροφορίας, των συστημάτων και των εφαρμογών, αποτελεί βασική απαίτηση κατά την ανάπτυξη και λειτουργία πληροφοριακών συστημάτων. Το μάθημα καλύπτει βασικά ζητήματα της ασφάλειας πληροφοριακών συστημάτων και περιλαμβάνει τις εξής ενότητες:

1. Εισαγωγικές έννοιες ασφάλειας συστημάτων.
2. Συστήματα Διαχείρισης Ασφάλειας.
3. Κρυπτογραφικά συστήματα.
4. Υποδομή Δημόσιας Κλείδας.
5. Έλεγχος προσπέλασης – Ιδιωτικότητα.
6. Ασφάλεια στις Τεχνολογίες.
7. Ασφαλείς η/κ-υπηρεσίες.
8. Εισαγωγή στην ασφάλεια δικτύων

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μετά την ολοκλήρωση του μαθήματος οι φοιτητές θα είναι σε θέση:

- Να κατανοούν βασικές εννοιών ασφάλειας σε όλα τα επίπεδα των υπολογιστικών δικτύων με έμφαση στα **TCP/IP** δίκτυα.
- Να διακρίνουν τα τρωτά σημεία στα συστήματα αυτά.
- Να προβλέπουν τυχόν αδυναμίες και αστοχίες.
- Να αναζητούν και να εφευρίσκουν/ανακαλύπτουν τρόπους επίλυσης/διαχείρισης για την περιστολή των τρωτών σημείων.
- Να σχεδιάζουν, λαμβάνοντας υπόψη την ανάλυση των δεδομένων, νέες τεχνικές/μεθόδους.
- Να προχωρούν σε πρακτική εφαρμογή συστημάτων ασφάλειας δικτύων, με έμφαση στη χρήση ελεύθερου λογισμικού / λογισμικού ανοικτού κώδικα.

6.3.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

- Ασφάλεια σε διαφορετικά επίπεδα της διαστρωμάτωσης **OSI**, όπως
 - ο σε επίπεδο σύνδεσης (**layer 2**),
 - ο σε επίπεδο δικτύου (**layer 3**)
 - ο σε επίπεδο εφαρμογής (**application layer**).

- Πρωτόκολλα διαχείρισης κλειδιών και πρωτόκολλα διαχείρισης ταυτοτήτων.
 - Αναχώματα ασφάλειας (**firewalls**) και συστήματα αναγνώρισης εισβολέων.
 - Η έννοια της εμπιστοσύνης στα δίκτυα καθώς και η διαχείριση της.
- Συστήματα καταναμημένης αυθεντικοποίησης

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Στόχος του μαθήματος είναι η παρουσίαση και η ανάλυση των μέτρων που εφαρμόζονται σε μια δικτυακή υποδομή, των πολιτικών που υιοθετούνται από τον διαχειριστή του δικτύου για να προστατεύσουν το δίκτυο και τους πόρους του από μη εξουσιοδοτημένη πρόσβαση, καθώς και η αποτελεσματικότητα (ή η έλλειψη) αυτών. Το μάθημα εστιάζει στην ασφάλεια των ενούρματων – σταθερών δικτύων τα οποία χρησιμοποιούν την τεχνολογία του Διαδικτύου. Παρουσιάζονται και αναλύονται οι μηχανισμοί και τα πρωτόκολλα ασφάλειας που διασφαλίζουν τη λειτουργία των παραπάνω δικτύων καθώς και τα δεδομένα των χρηστών τους.

Με την επιτυχή ολοκλήρωση του μαθήματος ο φοιτητής / τρια θα έχει εξοικειωθεί και θα εφαρμόζει διαφορετικά μέτρα και τεχνικές ασφάλειας που εφαρμόζονται στα ενούρματα δίκτυα τα οποία έχουν σαν στόχο να παρέχουν υπηρεσίες ασφάλειας στους χρήστες ενός δικτύου καθώς και στους παρόχους αυτού. [10]

7. ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

7.ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

7.1 ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

7.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

- Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας. Έλεγχος Πρόσβασης.
- Ταυτοποίηση και Αυθεντικοποίηση. Αρχές Κρυπτογραφίας και Κρυπτανάλυσης.
- Συμμετρική και Ασύμμετρη Κρυπτογραφία. Πιστοποιητικά. Ψηφιακές Υπογραφές.
- Ασφάλεια Λειτουργικών Συστημάτων, Βάσεων Δεδομένων και Δικτύων.
- Κακόβουλο Λογισμικό. Υπηρεσίες Διαδικτύου και Ασφάλεια. Τεχνολογίες Εμπιστοσύνης.
- Ζητήματα Ασφάλειας στο Απανταχού Υπολογίζειν Υποδομές Πλέγματος και Υπολογιστικού Σύννεφου, Διαδίκτυο Πραγμάτων.
- Εφαρμογές-Μελέτη Περιπτώσεων

- Προσωπικά Δεδομένα. Ιδιωτικότητα. Νομικό Πλαίσιο σε εθνικό και ευρωπαϊκό επίπεδο και Ηθικά Ζητήματα.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Με την επιτυχή ολοκλήρωση του μαθήματος ο φοιτητής / τρια θα έχει:

- Επαφή με τη διεπιστημονική τεχνολογική, οικονομική, νομική, κοινωνική οριοθέτηση της ασφάλειας, της εμπιστοσύνης και της ιδιωτικότητας
- Εξοικείωση με τα ζητήματα ασφάλειας και τις συμμετέχουσες τεχνολογίες στα σύγχρονα πληροφοριακά συστήματα
- Κατανόηση και δυνατότητα ανάλυσης ευπαθειών, απειλών και επιπτώσεων επιθέσεων στα πληροφοριακά συστήματα
- Αποκτήσει τα απαραίτητα εφόδια για τη θωράκιση του πληροφοριακού συστήματος από απειλές και κινδύνους. [11]

8. ΕΘΝΙΚΟ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

8.1 ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

8.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγή στην ασφάλεια. Βασικοί ορισμοί, συνηθισμένες απειλές στην ασφάλεια, ειδικές απαιτήσεις για δικτυακά περιβάλλοντα.
- Προσεγγίσεις στην επίτευξη ασφάλειας.
- Μηχανισμοί προστασίας, διακρίβωση ταυτότητας, έλεγχος προσπέλασης, τεχνικές διασφάλισης. Προστασία υπολογιστικών πόρων στο διαδίκτυο.
- **Firewalls**, περιτυλίγματα υπηρεσιών και συναφείς τεχνικές.
- Εισαγωγή στην κρυπτογραφία και τη διαχείριση κλειδιών.
- Κρυπτογραφία, συμμετρικοί και ασύμμετροι αλγόριθμοι, διακρίβωση δημόσιων κλειδιών, διαχείριση κλειδιών, ψηφιακές υπογραφές, αναφορές σε τεχνικές κρυπτανάλυσης.
- Ασφάλεια χρηστών στο διαδίκτυο. Κίνδυνοι από ενεργό περιεχόμενο που διακινείται στο διαδίκτυο και τρόποι προστασίας.
- Πλαίσιο ασφάλειας για τις γλώσσες **Javascript** και **Java**. Το πρόβλημα των ιών.
- Τι είναι ιός, είδη ιών, τρόποι μόλυνσης, τεχνικές που χρησιμοποιούν οι ιοί, λογισμικό και μέθοδοι αντιμετώπισης των ιών. Εργαλεία ανίχνευσης ευπαθειών.
- Γενικοί ορισμοί, ο ρόλος τους, μέθοδοι ελέγχου, παραδείγματα. Συστήματα ανίχνευσης εισβολών.

- Λόγοι χρήσης, γενικό μοντέλο, αρχιτεκτονική των συστημάτων, ειδικά χαρακτηριστικά και τεχνικές, τρόποι αντίδρασης. [18]

9. ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΗΣΟΥ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

9.1 ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

9.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Περιεχόμενα:

- Εισαγωγή (επιθέσεις, υπηρεσίες και μηχανισμοί ασφάλειας),
- Βασικά θέματα κρυπτογραφίας (συμμετρική κρυπτογραφία, ασύμμετρη κρυπτογραφία, συναρτήσεις σύννοψης),
- Υποδομές δημοσίων κλειδιών (ψηφιακές υπογραφές, ψηφιακά πιστοποιητικά και πρότυπα, έμπιστες τρίτες οντότητες, αρχιτεκτονικές, τεχνολογίες-πρότυπα),
- Πιστοποίηση ταυτότητας , ασφάλεια στον προγραμματισμό, προστασία πόρων στο διαδίκτυο,
- Ασφάλεια στο διαδίκτυο, ασφάλεια λειτουργικών συστημάτων, ασφάλεια συστημάτων βάσεων δεδομένων, ιοί, συστήματα ανίχνευσης εισβολών.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Στο τέλος του μαθήματος ο φοιτητής θα μπορεί να:

- περιγράφει βασικές αρχές των υπηρεσιών και μηχανισμών για τη διασφάλιση της εμπιστευτικότητας και ακεραιότητας
- εφαρμόζει τρόπους διασφάλισης της πληροφορίας στα περισσότερα επίπεδα του μοντέλου **OSI**
- αποτιμά τις επιπτώσεις, όσον αφορά την ασφάλεια, των επιλογών παραμετροποίησης σε μηχανισμούς ασφάλειας
- περιγράφει βασικές τεχνικές επιθέσεων και των αδυναμιών που εκμεταλλεύονται. [12]

10. ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

10.1 ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

10.2 ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

10.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα κατά το πρόγραμμα σποδών είναι υποχρεωτικό κατά τη διάρκεια της φοίτησης.

- Εισαγωγικές έννοιες ασφάλειας συστημάτων
- Απαιτήσεις Ασφάλειας κατά **ISO 27001**
- Πολιτικές και Διαδικασίες Ασφάλειας
- Μεθοδολογίες και Εργαλεία Ανάλυσης Επικινδυνότητας (**Risk Assessment Methodologies and Tools**)
- Υπηρεσίες Αυθεντικοποίησης
- Υπηρεσίες Εξουσιοδότησης
- Βασικοί αλγόριθμοι κρυπτογράφησης.
- Βασικές Αρχές Ασφάλειας Δικτύου
- Ασφάλεια Λειτουργικών Συστημάτων
- Απειλές **Web** Εφαρμογών
- Τεχνικές, εργαλεία και μεθοδολογίες ανίχνευσης αδυναμιών

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Το μάθημα αυτό έχει σαν στόχο να εφοδιάσει τους προπτυχιακούς φοιτητές με όλες τις θεμελιώδεις γνώσεις που θα τους επιτρέψουν να παρακολουθούν τις εξελίξεις που συντελούνται στον τομέα της Ασφάλειας Πληροφοριακών Συστημάτων.

Το μάθημα αποτελεί μια εισαγωγή στα προβλήματα ασφάλειας και Διαχείρισης Δικτύων.

Τα θέματα που καλύπτει μεταξύ άλλων είναι η εισαγωγή στην Ασφάλεια Δικτύων,

Η Αρχιτεκτονική Ασφάλειας Δικτύων **ISO/OSI**, η Αρχιτεκτονική και Μηχανισμοί ασφάλειας του Internet πρωτοκόλλου, Τεχνολογίες Ανίχνευσης

Δικτύων, Συστήματα Ανίχνευσης Εισβολών, Συστήματα Αυθεντικοποίησης σε Κατανεμημένα Περιβάλλοντα, Ασφάλεια σε ασύρματα δίκτυα, Εισαγωγή στην Διαχείριση Δικτύων, Ασφαλή Διαχείριση Δικτύων και λογισμικό διαχείρισης.

Κύριοι στόχοι του μαθήματος είναι οι ακόλουθοι:

- Η κατανόηση των απαιτήσεων των προτύπων διαχείρισης ασφάλειας πληροφοριών
- Η εξοικείωση με τις μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας
- Η εξοικείωση με τις βασικές υπηρεσίες ασφάλειας (αυθεντικοποίηση, ταυτοποίηση κλπ.)
- Η κατανόηση των απειλών / αδυναμιών **web** εφαρμογών
- Η εξοικείωση με τις μεθοδολογίες και εργαλεία ανίχνευσης τεχνικών αδυναμιών σε επίπεδο δικτύου και web εφαρμογών (**web / network penetration testing**)

10.2.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα είναι επιλογής κατά την διάρκεια των σποδών

Τα περιεχόμενα του μαθήματος έχουν ως ακολούθως:

- Εισαγωγικές έννοιες, αρχιτεκτονικές δικτύων, επιθέσεις, υπηρεσίες και μηχανισμοί ασφάλειας.
- Κρυπτογραφικά εργαλεία, επαλήθευση χρήστη, έλεγχος πρόσβασης, κακόβουλο λογισμικό, επιθέσεις άρνησης υπηρεσίας, ανίχνευση επίθεσης, τείχη προστασίας (**firewalls**), μηχανισμοί πρόληψης.
- Συμμετρικοί κώδικες, στενογραφία, το πρότυπο **DES**, το πρότυπο **AES**, πολλαπλή κρυπτογράφηση και τριπλό **DES**, ασύμμετροι κώδικες, αρχές συστημάτων δημόσιου κλειδιού, αλγόριθμος **RSA**.
- Ακεραιότητα κρυπτογραφικών δεδομένων, συναρτήσεις κατατεμαχισμού (**hash**), **SHA**, επαλήθευση ταυτότητας μηνύματος (**MAC**), ψηφιακές υπογραφές.
- Αμοιβαία εμπιστοσύνη στο Διαδίκτυο, διανομή συμμετρικού κλειδιού, διανομή δημόσιων κλειδιών, υποδομή δημόσιου κλειδιού, απομακρυσμένη επαλήθευση ταυτότητας χρήστη, **Kerberos**, **X.509**.
- Ζητήματα ασφάλειας του Ιστού: στρώμα ασφαλών υποδοχών (**SSL**), ασφάλεια στρώματος μεταφοράς (**TLS**), ασφαλές πρωτόκολλο μεταφοράς υπερκειμένου (**HTTPS**), ασφαλής φλοιός (**SSH**).
- Ασφάλεια ασύρματων δικτύων, **IEEE 802.11i**, ασφάλεια σε επίπεδο μεταφοράς, ασφάλεια **WAP** μεταξύ άκρων.
- Ηλεκτρονική αλληλογραφία, **PGP**, **S/MIME**, **DKIM**. Ασφάλεια στο **IP**, ενθυλάκωση, ανταλλαγή κλειδιών, κρυπτογραφικές σουίτες. Το μάθημα ενδέχεται να περιλαμβάνει εργαστηριακές ασκήσεις στις εξής περιοχές: Αλγόριθμοι κρυπτογραφίας, συγκέντρωση πληροφοριών και ανίχνευση αδυναμιών, συστήματα ανίχνευσης εισβολής, τείχη προστασίας.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Αυτό το μάθημα προσφέρεται στο 8ο εξάμηνο του κύριου προγράμματος σπουδών και αποσκοπεί στην παροχή βασικών γνώσεων σχετικά με τις αρχές που διέπουν την Ασφάλεια Δικτύων Υπολογιστών. Με την ολοκλήρωση αυτού του μαθήματος, οι φοιτητές/τριες θα έχουν μια βαθύτερη κατανόηση του τι είναι Ασφάλεια Δικτύων Υπολογιστών και διάφορες τεχνολογίες που την εξασφαλίζουν. Στο τέλος του μαθήματος ο φοιτητής / τρια θα είναι σε θέση να:

- Αναγνωρίζει βασικές αδυναμίες ασφάλειας στο επίπεδο του λογισμικού, του υλικού, του δικτύου και του ολοκληρωμένου συστήματος.
- Αντιλαμβάνεται τους μηχανισμούς μέσω των οποίων φαινομενικά αθώα σφάλματα ή αβλεψίες κατά την υλοποίηση και τη σχεδίαση υπολογιστικών συστημάτων μπορούν να οδηγήσουν σε εκμεταλλεύσιμες αδυναμίες.
- Γνωρίζει και είναι σε θέση να εφαρμόσει συνήθεις επιθέσεις (παραδοσιακές αλλά και πρόσφατες) οι οποίες εκμεταλλεύονται τις παραπάνω αδυναμίες.
- Γνωρίζει και είναι σε θέση να εφαρμόσει τις τεχνικές άμυνας έναντι των παραπάνω αδυναμιών / επιθέσεων.
- Σχεδιάζει συστήματα ακολουθώντας καλές πρακτικές στον τομέα της ασφάλειας.
- Ερμηνεύσει τη συμπεριφορά του συστήματος χρησιμοποιώντας επιστημονικά αποδεκτές μεθοδολογίες και να καταγράψει τις παρατηρήσεις σε τεχνική αναφορά. [13]

11.ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΒΙΟΙΑΤΡΙΚΗ

11.1 ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

11.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγή στην ασφάλεια υπολογιστών, κρυπτογραφία, έλεγχος πρόσβασης,
- Ασφάλεια βάσεων δεδομένων, κακόβουλο λογισμικό, επιθέσεις άρνησης εξυπηρέτησης
- ανίχνευση εισβολών, τείχη προστασίας και συστήματα αποτροπής
- εισβολών, υπερχειλίση περιοχής προσωρινής αποθήκευσης, ασφάλεια λογισμικού,
- ασφάλεια λειτουργικών συστημάτων, έμπιστη υπολογιστική, διαχείριση ασφάλειας
- και εκτίμηση κινδύνου, μηχανισμοί ελέγχου, σχέδια και διαδικασίες της ασφάλειας,

- ασφάλεια ανθρωπίνων πόρων, διαχειριστική παρακολούθηση της ασφάλειας,
- πρωτόκολλα και πρότυπα ασφάλειας του διαδικτύου, εφαρμογές πιστοποίησης ταυτότητας μέσω του διαδικτύου, ασφάλεια ασυρμάτων δικτύων.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Στόχος του μαθήματος είναι η εξοικείωση των φοιτητών με τις έννοιες της ασφάλειας και της ιδιωτικότητας σχετικά με τα συστήματα και τα δίκτυα υπολογιστών. Το μάθημα παρέχει τόσο το θεωρητικό υπόβαθρο όσο και τις απαραίτητες πρακτικές εφαρμογές της επιστημονικής περιοχής της ασφάλειας υπολογιστών. Έτσι οι φοιτητές είναι σε θέση να εφαρμόσουν τις αποκτώμενες γνώσεις τόσο σε ακαδημαϊκό όσο και οποιοδήποτε άλλο εργασιακό περιβάλλον. Με την επιτυχή ολοκλήρωση του μαθήματος οι φοιτητές θα πρέπει να είναι ικανοί:

- Να αντιλαμβάνονται τις βασικές έννοιες σχετικά με την ασφάλεια υπολογιστικών συστημάτων
- Να αναγνωρίζουν τις συνηθέστερες απειλές ασφαλείας
- Να γνωρίζουν τις τεχνικές αντιμετώπισης των συνηθέστερων απειλών και να μπορούν να τις χρησιμοποιήσουν.
- Να μπορούν να χρησιμοποιήσουν τις τεχνολογίες παρακολούθησης και διαχείρισης της ασφάλειας ενός συστήματος
- Να αντιλαμβάνονται την λειτουργία των συνηθέστερα χρησιμοποιούμενων πρωτοκόλλων ασφαλείας[14]

Στο κεφάλαιο εκτός από αυτά τα Πανεπιστημιακά ιδρύματα που παρουσιάζαμε παραπάνω στο μάθημα της ασφάλειας των πληροφοριακών συστημάτων θα παρουσιάσουμε και τις Σχολές Μηχανικών Πληροφορικής και στο τι διεξάγεται σε κάθε τμήμα ξεχωριστά τα οποία είναι τα εξής:

1. ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

1.1 ΜΑΘΗΜΑ : ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

1.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

- **Εισαγωγή στην ασφάλεια:** ασφάλεια υπολογιστών, μοντέλο ασφάλειας, επιθέσεις, αρχιτεκτονική ασφάλειας **OSI**, λειτουργικές απαιτήσεις και στρατηγική

- **Συμμετρική κρυπτογραφία:** ορισμοί, απαντήσεις, δομή **Feistel**, **DES**, **3DES**, **AES**, κωδικοποιητές ροής, **modes** κρυπτογράφησης μπλοκ, διανομή μυστικών κλειδιών
- **Στοιχεία θεωρίας αριθμών:** παράδοξο γενεθλίων, διαιρετότητα και πρώτοι αριθμοί, συνάρτηση **Totient** του **Euler**, αλγόριθμος του Ευκλείδη
- **Κρυπτογραφία δημόσιου κλειδιού:** βήματα, απαντήσεις, **RSA**, **Diffie-Hellman**, έλεγχος αυθεντικότητας μηνύματος, κώδικας ελέγχου αυθεντικότητας μηνύματος (**MAC**), μονόδρομη συνάρτηση κατακερματισμού (**SHA-1**, **SHA-512**, **MD5**), μέθοδος **HMAC**, ψηφιακές υπογραφές
- **Ασφάλεια λογισμικού:** επίθεση υπερχειλίσσης στοίβας, **shellcode**, ασφαλείς τεχνικές προγραμματισμού, αμυντικός προγραμματισμός, ένθεση εντολών, **cross-site scripting (XSS)**, **time-of-check-to-time-of-use (TOCTOU)**
- **Ασφάλεια υπολογιστικών συστημάτων:** έλεγχος πρόσβασης, διακριτικός έλεγχος πρόσβασης, έλεγχος πρόσβασης με ρόλους, υποχρεωτικός έλεγχος πρόσβασης (**Bell-Lapadula**, **Biba**), έμπιστος υπολογισμός, **trusted platform module**
- **Ασφάλεια δικτύων:** άρνηση εξυπηρέτησης (**denial of service**), **spoofing**, αντανάκλαση, τείχος προστασίας (**firewall**), **network address translation (NAT)**
- **Ασφάλεια διαδικτύου:** πρωτόκολλο **IPSec**, συσχέτιση ασφάλειας, **authentication header** και **encapsulating security payload**, κατάσταση μεταφοράς και σήραγγας
- **Ασφάλεια ιστού:** πρωτόκολλο ασφαλούς επικοινωνίας στον παγκόσμιο ιστό (**SSL/TLS**), πρωτόκολλο ασφαλούς χρήσης πιστωτικών καρτών στο διαδίκτυο (**SET**)
- **Κατανεμημένος έλεγχος αυθεντικότητας:** πρωτόκολλο **Kerberos**, υπηρεσία ελέγχου αυθεντικότητας **X.509**
- **Αλυσίδες μπλοκ και κρυπτονομίσματα:** μπλοκ, αλυσίδα μπλοκ, διεύθυνση, συναλλαγή, συναίνεση, **proof of work**, εξόρυξη

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Το μάθημα στοχεύει να διδάξει βασικές μεθόδους κρυπτογράφησης, αρχές ασφάλειας συστημάτων και λογισμικού, ασφαλή πρωτόκολλα για το διαδίκτυο και τον παγκόσμιο ιστό, εφαρμοσμένη προγραμματιστική εμπειρία σε επιθέσεις λογισμικού και δικτύων.

[15]

2. ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

2.1 ΜΑΘΗΜΑ : ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

2.2 ΜΑΘΗΜΑ : ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

2.3 ΜΑΘΗΜΑ : ΣΥΓΧΡΟΝΕΣ ΕΦΑΡΜΟΓΕΣ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

2.4 ΜΑΘΗΜΑ : ΑΣΦΑΛΕΙΑ ΣΕ ΥΛΙΚΟ

2.2.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα κατά την διάρκεια των σπουδών είναι υποχρεωτικό

- Αρχές ανάλυσης, σχεδίασης και υλοποίησης συστημάτων ασφαλείας υπολογιστών και δικτύων.
- Αρχιτεκτονική στρατιωτικών και εμπορικών ασφαλών συστημάτων. Δημιουργία ψευδοτυχαίων αριθμών.
- Συμμετρική κρυπτογραφία.
- Κρυπτογραφία δημόσιου κλειδιού.
- Ψηφιακές υπογραφές και πιστοποιητικά.
- Κρυπτογραφικά πρωτόκολλα.
- Ασφάλεια υπολογιστικών συστημάτων.
- Ασφάλεια δικτύων.
- Ασφάλεια εφαρμογών.
- Αρχιτεκτονική κρυπτοσυστημάτων και συστημάτων ασφαλείας υπολογιστών και δικτύων.
- Θέματα υλοποίησης ασφαλών συστημάτων

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Περιγράφονται τα μαθησιακά αποτελέσματα του μαθήματος οι συγκεκριμένες γνώσεις, δεξιότητες και ικανότητες κατάλληλου επιπέδου που θα αποκτήσουν οι φοιτητές μετά την επιτυχή ολοκλήρωση του μαθήματος.

- Περιγραφή του Επιπέδου των Μαθησιακών Αποτελεσμάτων για κάθε ένα κύκλο σπουδών σύμφωνα με Πλαίσιο Προσόντων του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης
- Περιγραφικοί Δείκτες Επιπέδων 6, 7 & 8 του Ευρωπαϊκού Πλαισίου Προσόντων Διά Βίου Μάθησης
- Περιληπτικός Οδηγός συγγραφής Μαθησιακών Αποτελεσμάτων

Μετά το πέρας του μαθήματος ο/η φοιτητής/τρια μπορεί να:

- Εξηγήσει το ρόλο και την σημασία της ασφαλείας υπολογιστών και δικτύων

- Κατανοήσει τα βασικά χαρακτηριστικά κρυπτογραφικών αλγορίθμων
- Κατανοήσει και χρησιμοποιήσει συμμετρικούς κρυπτογραφικούς αλγόριθμους και αλγόριθμους δημόσιου κλειδιού
- Αναλύει και αποτιμά συστήματα ασφάλειας υπολογιστών
- Αναλύει και αποτιμά συστήματα ασφάλειας δικτύων
- Σχεδιάζει και υλοποιεί ασφαλή συστήματα και εφαρμογές Κρίνει τα πλεονεκτήματα και τα μειονεκτήματα εναλλακτικών αρχιτεκτονικών ασφάλειας

Γενικές Ικανότητες

Λαμβάνοντας υπόψη τις γενικές ικανότητες που πρέπει να έχει αποκτήσει ο πτυχιούχος (όπως αυτές αναγράφονται στο Παράρτημα Διπλώματος και παρατίθενται ακολούθως) σε ποια / ποιες από αυτές αποσκοπεί το μάθημα;

- | | |
|--|--|
| <ul style="list-style-type: none"> • Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών • Προσαρμογή σε νέες καταστάσεις • Λήψη αποφάσεων • Αυτόνομη εργασία • Ομαδική εργασία • Εργασία σε διεθνές περιβάλλον • Εργασία σε διεπιστημονικό περιβάλλον • Παραγωγή νέων ερευνητικών ιδεών | <ul style="list-style-type: none"> • Σχεδιασμός και διαχείριση έργων • Σεβασμός στη διαφορετικότητα και στην πολυπολιτισμικότητα • Σεβασμός στο φυσικό περιβάλλον • Επίδειξη κοινωνικής, επαγγελματικής και ηθικής υπευθυνότητας και ευαισθησίας σε θέματα φύλου • Άσκηση κριτικής και αυτοκριτικής • Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης |
|--|--|

2.2.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα κατά την διάρκεια της φοίτησης είναι επιλογής

- **Εισαγωγή στην ασφάλεια της πληροφορίας:**
- βασικές αρχές και καλές πρακτικές.
- Εφαρμοσμένη κρυπτογραφία.
- Διασφάλιση στο διαδίκτυο των πραγμάτων.
- Δικανική υπολογιστών.
- Ηθική στην κυβερνοασφάλεια και κυβερνοέγκλημα.
- Επιχειρησιακό πλάνο και διαχείριση πληροφορίας.
- Ασφαλές λογισμικό και διαδίκτυο.
- Ασφαλές υλικό.

- Κυβερνοασφάλεια και ενσωματωμένα συστήματα.
 - Διαχείριση κινδύνων πληροφορίας.
 - **Επιθέσεις:** λογισμικό και υλικό.
 - **Περιστατικά και κυβερνοχώρος:** ανάλυση και ανταπόκριση.
 - **Νέες έννοιες:** μηχανική μάθηση, τεχνητή νοημοσύνη, σκοτεινό διαδίκτυο.
- Προηγμένα συστήματα: παραδείγματα και εφαρμογές

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Περιγράφονται τα μαθησιακά αποτελέσματα του μαθήματος οι συγκεκριμένες γνώσεις, δεξιότητες και ικανότητες καταλλήλου επιπέδου που θα αποκτήσουν οι φοιτητές μετά την επιτυχή ολοκλήρωση του μαθήματος τα οποία είναι τα εξής:

- Περιγραφή του Επιπέδου των Μαθησιακών Αποτελεσμάτων για κάθε ένα κύκλο σπουδών σύμφωνα με Πλαίσιο Προσόντων του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης
- Περιγραφικοί Δείκτες Επιπέδων 6, 7 & 8 του Ευρωπαϊκού Πλαισίου Προσόντων Διά Βίου Μάθησης και Παράρτημα Β
- Περιληπτικός Οδηγός συγγραφής Μαθησιακών Αποτελεσμάτων

Ο φοιτητής, που ολοκληρώνει με επιτυχία το μάθημα, έχει την ικανότητα :

- να γνωρίζει το θεωρητικό υπόβαθρο της κυβερνοασφάλειας,
- σε σύγχρονες εφαρμογές και τεχνολογίες αιχμής ,
- να κατανοήσει την υλοποίηση της κυβερνοασφάλειας ως βασικό κριτήριο σχεδιασμού συστημάτων, τόσο σε υλικό όσο και σε λογισμικό,
- να έχει αποκτήσει τις βασικές γνώσεις της προστασίας, από παραβιάσεις και εισβολείς,
- να οδηγηθεί στη βέλτιστη κατανόηση των επιθέσεων σε εφαρμογές λογισμικού και σε διατάξεις υλικού και μέθοδοι προστασίας αυτών,
- να υλοποιήσει την ανίχνευση και απενεργοποίηση επιβλαβών λειτουργιών και κυκλωμάτων,
- να προσδιορίσει σύγχρονες και αναπτυσσόμενες έννοιες στην κυβερνοασφάλεια: μηχανική μάθηση, τεχνητή νοημοσύνη, σκοτεινό διαδίκτυο κ.α

2.3.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα κατά το πρόγραμμα σπουδών είναι επιλογής

- Εισαγωγή στην ασφάλεια δικτύων, Επιθέσεις στην ασφάλεια του δικτύου, επιθέσεις που στοχεύουν στην παρεμπόδιση των παρεχόμενων υπηρεσιών. Περιγραφή των βασικών υπηρεσιών και μηχανισμών ασφάλειας.

- Ευπάθειες **TCP / IP** και **DoS Attacks: IP Spoofing, SYN Flooding**, και **DoS** επιθέσεις.
- **DNS** και **DNS Cache Poisoning** επιθέσεις.
- Κρυπτογραφία δημόσιου κλειδιού και ο αλγόριθμος **RSA26**
- Προστασία από δικτυακές επιθέσεις: **Packet Filtering (Linux)** και **Proxy-Server Firewalls**.
- Πρωτόκολλα **PGP, IPSec, SSL/TLS, and Tor**
- Κακόβουλα **Malware: Viruses and Worms**
- Σάρωση θυρών και ευπαθειών, **Packet Sniffing**, Ανίχνευση εισβολών (**intrusions**) και δοκιμή επιθέσεων (**Penetration testing**) σε δικτυακά συστήματα.
- Επιθέσεις στο πρωτόκολλο Domain Name System (**DNS**) και Address Resolution Protocol (**ARP**)
- Τεχνολογίες Bots, Botnets, DDoS Attacks, and DDoS Attack Mitigation.
- Παρουσίαση και ανάλυση του κακόβουλου λογισμικού (**malicious software**) που συναντάται στο Διαδίκτυο.
- Επιθέσεις άρνησης παροχής υπηρεσιών στο Διαδίκτυο και τρόποι αντιμετώπισης τους.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Περιγράφονται τα μαθησιακά αποτελέσματα του μαθήματος οι συγκεκριμένες γνώσεις, δεξιότητες και ικανότητες καταλλήλου επιπέδου που θα αποκτήσουν οι φοιτητές μετά την επιτυχή ολοκλήρωση του μαθήματος. Συμβουλευτείτε το Παράρτημα Α

- Περιγραφή του Επιπέδου των Μαθησιακών Αποτελεσμάτων για κάθε ένα κύκλο σπουδών σύμφωνα με Πλαίσιο Προσόντων του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης
- Περιγραφικοί Δείκτες Επιπέδων 6, 7 & 8 του Ευρωπαϊκού Πλαισίου Προσόντων Διά Βίου Μάθησης και Παράρτημα Β
- Περιληπτικός Οδηγός συγγραφής Μαθησιακών Αποτελεσμάτων Ολοκληρώνοντας το μάθημα, οι φοιτητές θα είναι σε θέση:
- Να καθορίσουν τις πιθανές απειλές/κινδύνους δικτυακών συσκευών που ενδέχεται να επηρεάσουν τη λειτουργία, αποτελεσματικότητα, αποδοτικότητα και ιδιωτικότητα ενός δικτυακού συστήματος.
- Να χρησιμοποιούν εργαλεία και πρωτόκολλα ασφάλειας που ικανοποιούν καλά προσδιορισμένες απαιτήσεις και προστατεύουν από συγκεκριμένες απειλές.
- Να αξιολογήσουν την αποτελεσματικότητα και αποδοτικότητα μιας αρχιτεκτονικής ασφάλειας δικτύου αναγνωρίζοντας τις πιθανές αδυναμίες και περιορισμούς.
- Να γνωρίζουν τις τρέχουσες τάσεις κακόβουλων ενεργειών σε εξυπηρετητές

2.4.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα κατά το πρόγραμμα σπουδών είναι επιλογής

Θεωρητικό υπόβαθρο και βασικές αρχές: Ασφάλεια και εμπιστοσύνη σε συσκευές υλικού, και μελλοντικές εφαρμογές, νέες προκλήσεις,

- Βασικοί όροι: Κρυπτογραφία και ασφάλεια,
- Σχεδιασμός Ψηφιακών Συστημάτων,
- Αρχές και Μεθοδολογίες,
- Απόδοση υλικού,
- Φυσικές **Unclonable Functions (PUFs)**,
- Γεννήτριες τυχαίων και ψευδοτυχαίων αριθμών,
- Υδατοσήμανση και **IP** υλικού,
- Επιθέσεις: Ενέσεις σφαλμάτων, Φυσική, Αντίσταση παραβίασης,
- Επιθέσεις στα πλευρικά κανάλια: μοντέλα και αντίμετρα,
- Ασφάλεια ενσωματωμένων συστημάτων,
- Κρυπτοεπεξεργαστές,
- Ασφαλή σχέδια **FPGA**,
- Ασφάλεια ετικετών **RFID**

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Τα μαθησιακά αποτελέσματα του μαθήματος, συγκεκριμένες γνώσεις, δεξιότητες και ικανότητες κατάλληλου επιπέδου που θα αποκτήσουν οι φοιτητές με την επιτυχή ολοκλήρωση του μαθήματος περιγράφονται.

- Περιγραφή του επιπέδου των μαθησιακών αποτελεσμάτων για κάθε κύκλο προσόντων, σύμφωνα με το Πλαίσιο Προσόντων του Ευρωπαϊκός Χώρος Ανώτατης Εκπαίδευσης
- Περιγραφείς για τα Επίπεδα 6, 7 και 8 του Ευρωπαϊκού Πλαισίου Προσόντων για τη Δια Βίου Μάθηση
- Οδηγίες συγγραφής Μαθησιακών Αποτελεσμάτων[16]

3. ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

3.1 ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

3.2 ΑΣΦΑΛΕΙΑ ΚΙΝΗΤΩΝ ΚΑΙ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

3.3 ΑΣΦΑΛΕΙΑ ΣΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ

3.1.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα κατά το πρόγραμμα σπουδών είναι επιλογής

- Εννοιολογική Θεμελίωση όρων Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων.
- Ταυτοποίηση και Αυθεντικοποίηση.
- Έλεγχος Προσπέλασης.
- Πολιτικές και Φορμαλιστικά Μοντέλα Ασφάλειας. Ασφάλεια Λειτουργικών Συστημάτων, Μοντέλο περίπτωσης: Unix.
- Κακόβουλο Λογισμικό. Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας Πληροφοριακών Συστημάτων.
- Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων.
- Σειρά Προτύπων ISO 2700X. Στοιχεία Εφαρμοσμένης Κρυπτογραφίας: Κλασικές Κρυπτογραφικές Μέθοδοι,
- Συμμετρικά και Ασύμμετρα Κρυπτοσυστήματα, Κώδικες Αυθεντικοποίησης Μηνυμάτων, Ψηφιακές Υπογραφές,
- Πάροχοι Υπηρεσιών Πιστοποίησης, Υποδομή Δημόσιων Κλειδιών,
- Νομοθετικό και Ρυθμιστικό Πλαίσιο στην Ελλάδα. Ιδιωτικότητας.
- Ασφάλεια Δικτύων Υπολογιστών. Απειλές και Ευπάθειες. Αναχώματα Ασφάλειας. Αρχιτεκτονική Ασφάλειας στο μοντέλο του Internet. Εφαρμογές.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Σκοπός του μαθήματος είναι, μετά την ολοκλήρωση τη μαθησιακής διαδικασίας οι φοιτητές και φοιτήτριες να έχουν κατανοήσει με πληρότητα τα θεμελιώδη θέματα ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων και προστασίας της ιδιωτικότητας, να γνωρίζουν σε βάθος θέματα διοίκησης ασφάλειας πληροφοριακών συστημάτων στο πλαίσιο των προτύπων κατά ISO 2700X και να διαθέτουν βασικές γνώσεις θεμάτων ασφάλειας στο Διαδίκτυο και στοιχείων εφαρμοσμένης κρυπτογραφίας.

Με την επιτυχή ολοκλήρωση του μαθήματος οι φοιτητές:

- Θα έχουν κατανοήσει βασικές έννοιες ασφάλειας και μοντέλα ασφάλειας.
- Θα αποκτήσουν την ικανότητα εφαρμογής βασικών μεθόδων ανάλυσης επικινδυνότητας και χρήσης και αξιολόγησης βασικής τεχνολογίας ασφάλειας πληροφοριακών συστημάτων.

3.2.1 ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα είναι επιλογής κατά το πρόγραμμα σπουδών

- Εισαγωγή στην ασφάλεια ασύρματων επικοινωνιών: Συγκριτική θεώρηση ασφάλειας σε σχέση με τα ενσύρματα περιβάλλοντα, Κατηγορίες απειλών και **OSI**, Σημεία ευπάθειας, Αντίμετρα, Αρχιτεκτονικές ασφάλειας.
- Ζητήματα ασφάλειας στο πρότυπο **IEEE 802.11**: Μηχανισμοί πιστοποίησης ταυτότητας και εξουσιοδότησης, Πλαίσιο **IEEE 802.1X**, Εμπιστευτικότητα και Ακεραιότητα δεδομένων, **pre-RSNA (WEP)**, **TSNs (TKIP)**, **RSNA (802.11i)**, Διαχείριση κλειδιών, Ανάλυση απειλών και Περιγραφή επιθέσεων.
- **Ζητήματα ασφάλειας σε κινητά (κυψελωτά) δίκτυα επικοινωνιών:** Ασφάλεια σε περιβάλλοντα **2/2.5/3/4G (GSM, GPRS, UMTS, LTE)**, Πιστοποίηση ταυτότητας, Ιεραρχία και Διαχείριση κλειδιών, Ιδιωτικότητα, Ανωνυμία, Ενδοδικτυακή και Δια-δικτυακή ασφάλεια των δικτύων των παρόχων υπηρεσιών, Κατηγορίες επιθέσεων.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Η παρούσα διδακτική ενότητα εστιάζει σε εισαγωγικά θέματα Ασφάλειας Κινητών και Ασύρματων Δικτύων Επικοινωνιών. Αναλυτικότερα, οι βασικοί εκπαιδευτικοί στόχοι του μαθήματος είναι:

- Η απόκτηση και ανάπτυξη κουλτούρας ασφάλειας σε περιβάλλον κινητών και ασύρματων δικτύων επικοινωνιών.
- Η παρουσίαση και ανάλυση των διάφορων κατηγοριών απειλών, των σημείων ευπάθειας, των αντιμέτρων, και των μεθόδων διασφάλισης στις σημαντικότερες τεχνολογίες ασύρματων και κυψελωτών δικτύων επικοινωνιών.

Σε αυτό το πλαίσιο, οι φοιτητές γνωρίζουν τα βασικά χαρακτηριστικά ασφάλειας των κινητών επικοινωνιών 2ης, 3ης και 4ης γενιάς, καθώς και τα αντίστοιχα που αναπτύσσονται στα ασύρματα δίκτυα **IEEE 802.11**.

Η δεύτερη κύρια συνιστώσα του μαθήματος αναφέρεται στην απαίτηση της Ιδιωτικότητας για τους χρήστες των εν λόγω δικτύων.

Στόχος είναι η γνωριμία και εξοικείωση των φοιτητών και φοιτητριών με τη σχετική ορολογία και τις βασικές τεχνολογίες προστασίας της Ιδιωτικότητας σε περιβάλλον κινητών και ασύρματων δικτύων επικοινωνιών.

Ο στόχος των εργαστηριακών εφαρμογών και μελετών περίπτωσης είναι να βοηθήσουν τους φοιτητές να μάθουν να χρησιμοποιούν με βέλτιστο τρόπο τις παραπάνω τεχνολογίες ασφάλειας και διαφύλαξης της Ιδιωτικότητας σε περιβάλλον κινητών επικοινωνιών.

Ο πυρήνας των διδακτικών στόχων της παρούσας ενότητας είναι η εμπέδωση διαφορετικής κουλτούρας και αντίληψης ασφάλειας και Ιδιωτικότητας σε σχέση με το ενσύρματο δικτυακό περιβάλλον.

Σε αυτήν την κατεύθυνση, οι εργασίες του μαθήματος υλοποιούνται κάνοντας χρήση της πλατφόρμας **Google Android** ή/και **IOS**.

Με την επιτυχή ολοκλήρωση του μαθήματος ο φοιτητής/τρια θα είναι σε θέση να:

- Αντιλαμβάνεται την ιδιαιτερότητα των ασύρματων και κινητών δικτύων επικοινωνιών σε σχέση με τα ενσύρματα δίκτυα σε όρους ασφάλειας και ιδιωτικότητας.
- Γνωρίζει τις βασικές τεχνολογίες ασφάλειας και προστασίας της ιδιωτικότητας του χρήστη που παρέχονται από τα κυψελωτά δίκτυα επικοινωνιών και τα ασύρματα δίκτυα τεχνολογίας **IEEE 802.11**.
- Έχει κατανοήσει τους βασικούς τύπους επιθέσεων που μπορούν να εφαρμοστούν στους συγκεκριμένους τύπους δικτύων.
- Γνωρίζει τις βασικές αρχιτεκτονικές των δικτύων αυτού του τύπου.

3.3.3 ΠΕΡΙΦΡΑΦΗ ΜΑΘΗΜΑΤΟΣ

Το μάθημα είναι επιλογής κατά το πρόγραμμα σπουδών

- Εισαγωγή στην ασφάλεια προσεγγίζοντας την μέσα από τη θεωρία πληροφορίας.
- Βασικά στοιχεία θεωρίας πληροφορίας (πληροφορία, εντροπία, αμοιβαία πληροφορία, χωρητικότητα, **Gaussian** κανάλι, θεωρία ρυθμού παραμόρφωσης)
- Ορισμός ασφάλειας φυσικού επιπέδου. Μετρικά μυστικότητας και απορρήτου.
- Τέλεια μυστικότητα σε όρους θεωρίας πληροφορίας.
- Κανάλια υποκλοπής (**wiretap**). Χωρητικότητα μυστικότητας και χωρητικότητα μυστικού κλειδιού. Σύστημα κρυπτογράφησης **Shannon**.
- Όρια ασφάλειας διαύλων και ασύρματων καναλιών. Κωδικοποίηση για μυστικότητα. **Beamforming** και προ-κωδικοποίηση μυστικότητας, **MIMO** κανάλια.

- Βασικά στοιχεία για **Diffie-Hellman**, **AES** και επιθέσεις πλευρικού καναλιού. Χρήση από κοινού τυχαιότητας και τεχνητού θορύβου.
- Απόρρητο-παρεμβολή-jamming σε κανάλια πολλαπλών χρηστών. Ασφάλεια κωδικοποίησης δικτύου. **LDPC** κώδικες στο **wiretap** κανάλι.
- Γέννηση μυστικών κλειδιών, συμφωνία μυστικού κλειδιού (επικοινωνία μιας κατεύθυνσης, αμφίδρομη, και ανταλλαγή κβαντικών κλειδιών), **Fingerprinting** μέσω καναλιού. Κωδικοποίηση πηγής κάτω από περιορισμούς μυστικότητας.
- Επίλυση ασκήσεων μοντελοποίησης των καναλιών **wiretap**, εκτίμησης μυστικότητας, ανάπτυξης κωδικών και κωδικοποίησης, **beamforming** και γέννησης κλειδιών μέσω εκτίμησης καναλιού.

ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ

ΣΤΟΧΟΙ - ΕΠΙΔΙΩΚΟΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Με την επιτυχή ολοκλήρωση του μαθήματος, ο φοιτητής/τρια θα μπορεί:

- Να κατανοήσει βασικές μεθόδους ανάλυσης πληροφορίας,
- Να είναι σε θέση να ποσοτικοποιήσει την πληροφορία, τον ρυθμό πληροφορίας, να αξιολογεί την χωρητικότητα πληροφορίας στα κανάλια,
- Να εξοικειωθεί με τα μετρικά πληροφορίας και αβεβαιότητας,
- Να κατανοήσει τις βασικές αρχές επίτευξης ασφάλειας στο φυσικό επίπεδο και τα οφέλη και πλεονεκτήματα που προσφέρει,
- Να κατανοήσει τις έννοιες της μυστικότητας-απορρήτου, των μετρικών μυστικότητας και της χωρητικότητας απορρήτου/μυστικότητας,
- Να μελετήσει τα κανάλια υποκλοπών (**wiretap**) και να κατανοήσει τους κινδύνους αλλά και τα μέσα αποφυγής,
- Να μελετήσει το **beamforming**, την προ-κωδικοποίηση και τις συνεργατικές μορφές μετάδοσης ως μέσα απόρρητης και ασφαλούς επικοινωνίας,
- Να κατανοήσει τις διαδικασίες ασφαλούς κωδικοποίησης μέσου του καναλιού σε φυσικό επίπεδο[17]

ΚΕΦΑΛΑΙΟ 4: Στατιστικά Στοιχεία

ΠΑΡΟΥΣΙΑΣΗ ΣΤΑΤΙΣΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ ΕΡΕΥΝΑΣ

Η ερευνά μας που κάνουμε βασίζεται στα πανεπιστήμια που αναφέρθηκαν στο προηγούμενο κεφάλαιο αναλυτικά και παρακάτω θα διατυπώσουμε τα κριτήρια που κάνουμε την ερευνά μας είναι τα εξής:

1. Αν το μάθημα που αφορά την ασφάλεια των πληροφοριακών συστημάτων κάθε σχολής είναι υποχρεωτικό ή επιλογής.
1. Αν το μάθημα που αφορά την ασφάλεια των πληροφοριακών συστημάτων της του κάθε τμήματος έχουν εργαστηριακό μέρος.
2. Αν τα μαθήματα που είναι σε κάθε τμήμα και σχολή πληροφορικής διαφέρουν κατά την ύλη που διδάσκεται και τι διδάσκεται σε κάθε ένα ξεχωριστά.

Ο διαχωρισμός των σχολών πληροφορικής γίνεται σε 2 κατηγορίες:

3. Σε σχολές Πληροφορικής
4. Σε σχολές Μηχανικών πληροφορικής

Σύνολο Σχολών Πληροφορικής =14

ΣΥΝΟΛΟ ΟΛΩΝ ΤΩΝ ΜΑΘΗΜΑΤΩΝ=27

ΣΥΝΟΛΙΚΑ ΜΑΘΗΜΑΤΑ ΕΠΙΛΟΓΗΣ =17

-ΔΙΑΘΕΤΟΥΝ ΕΡΓΑΣΤΗΡΙΑΚΟ ΜΕΡΟΣ= 12

-ΔΕΝ ΔΙΑΘΕΤΟΥΝ ΕΡΓΑΣΤΗΡΙΑΚΟ ΜΕΡΟΣ = 5

ΣΥΝΟΛΙΚΑ ΜΑΘΗΜΑΤΑ ΠΟΥ ΕΙΝΑΙ ΥΠΟΧΡΕΩΤΙΚΑ =12

-ΔΙΑΘΕΤΟΥΝ ΕΡΓΑΣΤΗΡΙΑΚΟ ΜΕΡΟΣ = 9

-ΔΕΝ ΔΙΑΘΕΤΟΥΝ ΕΡΓΑΣΤΗΡΙΑΚΟ ΜΕΡΟΣ = 3

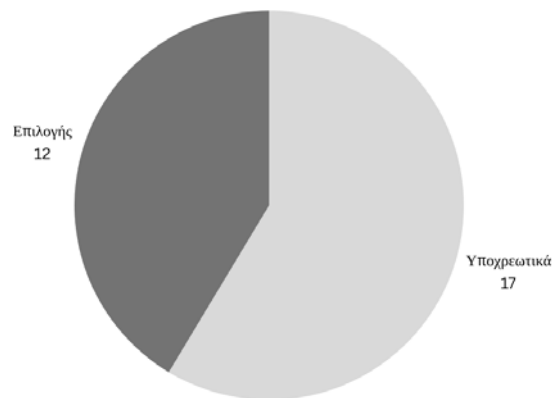
Επιστήμης Υπολογιστών (Ηράκλειο) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ	Εισαγωγή στα Συστήματα Ασφάλειας Πληροφοριών & Ψηφιακή Εγκληματολογία και Ασφάλεια	Επιλογής & Επιλογής		ΜΕ ΕΡΓΑΣΤΗΡΙΟ & ΜΕ ΕΡΓΑΣΤΗΡΙΟ
Εφαρμοσμένης Πληροφορικής (Θεσσαλονίκη) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ	ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ & ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΔΙΑΔΙΚΤΥΑΚΩΝ ΕΦΑΡΜΟΓΩΝ	Υποχρεωτικό & Επιλογής	Ασφάλεια Πληροφοριακών Συστημάτων (2,3,5,6,7,9,11,14) Ασφάλεια Δικτύων(2,3,4,5,6,9, 13,14)	ΜΕ ΕΡΓΑΣΤΗΡΙΟ & ΜΕ ΕΡΓΑΣΤΗΡΙΟ
Πληροφορικής (Αθήνα) - ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ	Ασφάλεια Πληροφοριακών Συστημάτων & Ασφάλεια Δικτύων	Υποχρεωτικό & Επιλογής	Ασφάλεια Πληροφοριακών Συστημάτων (2,3,5,6,7,9,11,14) Ασφάλεια Δικτύων(2,3,4,5,6,9, 13,14)	ΧΩΡΙΣ ΕΡΓΑΣΤΗΡΙΟ & ΜΕ ΕΡΓΑΣΤΗΡΙΟ
Πληροφορικής (Θεσσαλονίκη) - ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ	Ασφάλεια Δικτύων	Υποχρεωτικό	Ασφάλεια Δικτύων(2,3,4,5,6,9, 13,14)	ΜΕ ΕΡΓΑΣΤΗΡΙΟ
Πληροφορικής (Κέρκυρα) - ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ	Ασφάλεια Υπολογιστών και Προστασία Δεδομένων & Ασφάλεια Δικτύων Υπολογιστών και Επικοινωνιών & Ασφάλεια Λογισμικού και Εφαρμογών & Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων	Υποχρεωτικό & Επιλογής & Επιλογής & Επιλογής	Ασφάλεια Πληροφοριακών Συστημάτων (2,3,5,6,7,9,11,14) Ασφάλεια Δικτύων(2,3,4,5,6,9, 13,14)	ΜΕ ΕΡΓΑΣΤΗΡΙΟ & ΜΕ ΕΡΓΑΣΤΗΡΙΟ & ΜΕ ΕΡΓΑΣΤΗΡΙΟ & ΧΩΡΙΣ ΕΡΓΑΣΤΗΡΙΟ
Πληροφορικής (Πειραιάς) -	Διοίκηση Ασφάλειας Συστημάτων &	Επιλογής &	Ασφάλεια Πληροφοριακών Συστημάτων (2,3,5,6,7,9,11,14)	ΧΩΡΙΣ ΕΡΓΑΣΤΗΡΙΟ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ	ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ & Ασφάλεια Δικτύων	Υποχρεωτικό & Υποχρεωτικό	Ασφάλεια Δικτύων(2,3,4,5,6,9, 13,14)	& ΜΕ ΕΡΓΑΣΤΗΡΙΟ & ΜΕ ΕΡΓΑΣΤΗΡΙΟ
Πληροφορικής και Τηλεματικής (Αθήνα) - ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ	ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ	Υποχρεωτικό	Ασφάλεια Πληροφοριακών Συστημάτων (2,3,5,6,7,9,11,14)	ΧΩΡΙΣ ΕΡΓΑΣΤΗΡΙΟ
Πληροφορικής και Τηλεπικοινωνιών (Αθήνα) - ΕΘΝΙΚΟ & ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ	Προστασία και Ασφάλεια Υπολογιστικών Συστημάτων	Υποχρεωτικό		ΜΕ ΕΡΓΑΣΤΗΡΙΟ
Πληροφορικής και Τηλεπικοινωνιών (Λαμία) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ	ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ & ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ	Υποχρεωτικό & Επιλογής	Ασφάλεια Πληροφοριακών Συστημάτων (2,3,5,6,7,9,11,14) Ασφάλεια Δικτύων(2,3,4,5,6,9, 13,14)	ΜΕ ΕΡΓΑΣΤΗΡΙΟ & ΧΩΡΙΣ ΕΡΓΑΣΤΗΡΙΟ
Πληροφορικής και Τηλεπικοινωνιών (Τρίπολη) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ	Ασφάλεια συστημάτων	Επιλογής	Ασφάλεια Πληροφοριακών Συστημάτων (2,3,5,6,7,9,11,14)	ΜΕ ΕΡΓΑΣΤΗΡΙΟ
Πληροφορικής με Εφαρμογές στη Βιοϊατρική (Λαμία) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ	ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ	Υποχρεωτικό	Ασφάλεια Πληροφοριακών Συστημάτων (2,3,5,6,7,9,11,14)	ΧΩΡΙΣ ΕΡΓΑΣΤΗΡΙΟ

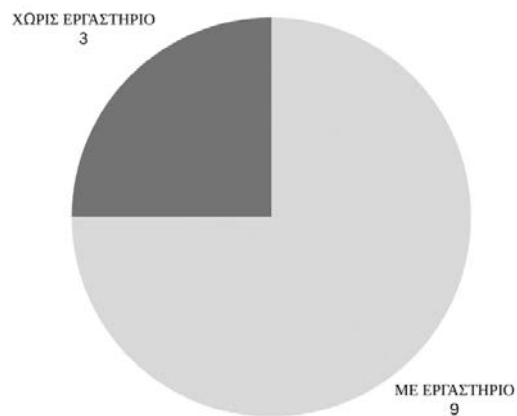
ΠΙΝΑΚΑΣ 1: ΑΠΟΤΕΣΜΑΤΑ ΑΠΟ ΤΗΝ ΕΡΕΥΝΑ ΤΟΝ ΠΑΝΕΠΙΣΤΗΜΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής (Ιωάννινα) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ	Ασφάλεια Υπολογιστικών και Επικοινωνιακών Συστημάτων	Υποχρεωτικό	Ασφάλεια Πληροφορια κών Συστημάτων (2,3,5,6,7,9,1 1,14)	ΜΕ ΕΡΓΑΣΤΗΡΙΟ
Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής (Πάτρα) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ	ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ & ΚΥΒΕΡΝΟΑΣΦΑ ΛΕΙΑ & Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων & ΑΣΦΑΛΕΙΑ ΣΕ ΥΛΙΚΟ	Επιλογής όλα	Ασφάλεια Δικτύων(2,3, 4,5,6,9,13,14)	ΧΩΡΙΣ ΕΡΓΑΣΤΗΡΙΟ & ΜΕ ΕΡΓΑΣΤΗΡΙΟ & ΜΕ ΕΡΓΑΣΤΗΡΙΟ & ΜΕ ΕΡΓΑΣΤΗΡΙΟ
Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων (Σάμος) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ	Ασφάλεια Πληροφοριακών & Επικοινωνιακών Συστημάτων & Ασφάλεια Δικτύων Υπολογιστών και Τεχνολογίες Προστασίας της Ιδιωτικότητας & Ασφάλεια Κινητών και Ασύρματων Δικτύων Επικοινωνιών & Ασφάλεια στο Φυσικό Επίπεδο	Υποχρεωτικό & Επιλογής & Επιλογής & Επιλογής	Ασφάλεια Πληροφορια κών Συστημάτων (2,3,5,6,7,9,1 1,14) Ασφάλεια Δικτύων(2,3, 4,5,6,9,13,14)	ΜΕ ΕΡΓΑΣΤΗΡΙΟ & ΧΩΡΙΣ ΕΡΓΑΣΤΗΡΙΟ & ΧΩΡΙΣ ΕΡΓΑΣΤΗΡΙΟ & ΧΩΡΙΣ ΕΡΓΑΣΤΗΡΙΟ
Σχολές	Μαθήματα ασφάλειας ανά σχολή	Επιλογής υποχρεωτικ ά μαθήματα	Κοινά μαθήματα στο πρόγραμμα σπουδών	Σε ποσά μαθήματα υπάρχουν εργαστήρια/φροντιστήρι α και σε ποσά όχι

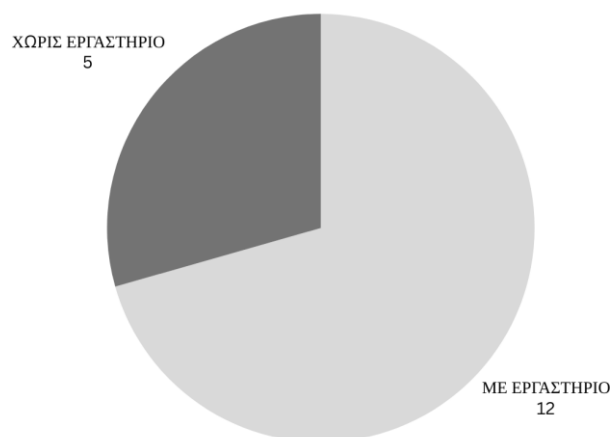
**ΠΙΝΑΚΑΣ 2 : ΑΠΟΤΕΣΜΑΤΑ ΑΠΟ ΤΗΝ ΕΡΕΥΝΑ ΤΟΝ ΠΑΝΕΠΙΣΤΗΜΙΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ**



ΓΡΑΦΗΜΑ ΠΙΤΑΣ 1 : ΑΝΑΠΑΡΑΣΤΑΣΗ ΤΩΝ ΜΑΘΗΜΑΤΩΝ ΕΠΙΛΟΓΗΣ ΚΑΙ ΤΩΝ ΥΠΟΧΡΕΩΤΙΚΩΝ



ΓΡΑΦΗΜΑ ΠΙΤΑΣ 2 : ΑΝΑΠΑΡΑΣΤΑΣΗ ΤΩΝ ΜΑΘΗΜΑΤΩΝ ΕΠΙΛΟΓΗΣ ΠΟΥ ΔΙΑΘΕΤΟΥΝ ΕΡΓΑΣΤΗΡΙΑΚΟ ΜΕΡΟΣ ΚΑΙ ΠΟΙΑ ΔΕΝ ΔΙΑΘΕΤΟΥΝ



ΓΡΑΦΗΜΑ ΠΙΤΑΣ 3: ΑΝΑΠΑΡΑΣΤΑΣΗ ΤΩΝ ΥΠΟΧΡΕΩΤΙΚΩΝ ΠΟΥ ΔΙΑΘΕΤΟΥΝ ΕΡΓΑΣΤΗΡΙΑΚΟ ΜΕΡΟΣ ΚΑΙ ΠΟΙΑ ΔΕΝ ΔΙΑΘΕΤΟΥΝ

ΚΕΦΑΛΑΙΟ 5

ΑΠΟΤΕΛΕΣΜΑΤΑ -ΣΥΜΠΕΡΑΣΜΑΤΑ

Σύμφωνα με την έρευνα μας οι συγκρίσεις και διαφορές μεταξύ των σχολών Πανεπιστημίου και των Πολυτεχνικών σχολών στον τομέα της πληροφορικής μπορούμε να διατυπώσουμε τα εξής συμπεράσματα :

➤ **Διαφοροποίηση μεταξύ Σχολών Πληροφορικής και Μηχανικών Πληροφορικής:**

Στις σχολές μηχανικών πληροφορικής φαίνεται να υπάρχει μεγαλύτερη έμφαση σε πιο τεχνικά και εξειδικευμένα θέματα ασφαλείας, όπως ασφάλεια στο υλικό και ασφάλεια κινητών και ασύρματων δικτύων.

➤ **Υποχρεωτικά & Επιλογής:**

Παρατηρείται μια ισορροπία μεταξύ υποχρεωτικών και μαθημάτων επιλογής. Αρκετές σχολές προσφέρουν τουλάχιστον ένα υποχρεωτικό μάθημα, ενώ άλλες εστιάζουν περισσότερο σε μαθήματα επιλογής.

➤ **Ύλη στα Πανεπιστήμια & Ύλη στις Πολυτεχνικές σχολές :**

Παρατηρούμε ότι σε κάθε τμήμα ξεχωριστά από αυτά που εξετάζουμε η ύλη που διδάσκετε είτε αυτό είναι Πανεπιστήμιο η Πολυτεχνική σχολή διαφέρει αρκετά σε μεγάλο βαθμό και στο που στοχεύει κάθε μάθημα που αφορά τον τομέα της ασφαλείας που εξετάζουμε.

➤ **Ειδίκευση στην Ασφάλεια:** Μεγάλο μέρος των μαθημάτων επικεντρώνεται στην ασφάλεια, με τονίσεις σε διάφορες πτυχές, όπως ασφάλεια δικτύων, ασφάλεια συστημάτων, κυβερνοασφάλεια και προστασία δεδομένων.

Πιο συγκεκριμένα, διακρίνουμε τις εξής διαφορές και συγκρίσεις μεταξύ των Πανεπιστημίων και των Πολυτεχνικών Σχολών:

➤ **Μαθήματα με Εργαστήριο:** Υπάρχει μια σημαντική προτίμηση για μαθήματα με εργαστήριο. Η πλειονότητα των μαθημάτων προσφέρει εργαστήριο, εκτός από κάποια ειδικά, όπως "Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων" στην Κέρκυρα και "Ασφάλεια Πληροφοριακών Συστημάτων" στην Αθήνα.

➤ **Μαθήματα χωρίς Εργαστήριο :** Κατά την διάρκεια των σπουδών παρατηρούμε ότι σε κάποια μαθήματα ενώ απαιτείται πρακτική εξάσκηση πάνω στο μάθημα είτε αυτό είναι επιλογής είτε είναι υποχρεωτικό δεν παρέχετε εργαστήριο για την ανάπτυξη δεξιοτήτων όπως ‘ Ασφάλεια

Δικτύων' στο Θεσσαλονίκη και 'Ασφάλεια Υπολογιστών Και Δικτυών' στην Πάτρα.

- Παρατηρούμε ότι υπάρχουν σε 2 σχολές υπάρχουν μαθήματα τα οποία είναι πιο κοντά στην ουσιαστική εφαρμογή στην παρούσα εποχή, όπως είναι το μάθημα “Ψηφιακή Εγκληματολογία Και Ασφάλεια” στο Ηράκλειο Κρήτης και “Σύγχρονες Εφαρμογές Ασφαλείας Δικτύων” στην Πάτρα.
- Παρατηρούμε ότι η Πολυτεχνική Σχολή των Πατρών παρέχει το μεγαλύτερο ποσοστό μαθημάτων επιλογής που 3 από αυτά παρέχουν και εργαστηριακό μέρος για την εξοικείωση όσον μαθαίνονται στο θεωρητικό κομμάτι των μαθημάτων.
- Ένα άλλο φαινόμενο που παρατηρείτε είναι ότι το μάθημα που αφορά την ασφάλειας τόσο των πληροφοριακών συστημάτων , των δικτύων και των προσωπικών δεδομένων ότι εμφανίζεται κατά βάση ως μαθήματα επιλογής και όχι ως υποχρεωτικό κατά την διάρκεια των σπουδών.
- Μπορούμε να παρατηρήσουμε ότι υπάρχει έντονη ομοιομορφία σε κάθε πανεπιστημιακό τμήμα, η πολυτεχνική σχολή έχει ως εικόνα των μαθημάτων επιλογής αλλά εξαιρούνται τα μαθήματα κορμού-υποχρεωτικά που συνεχίζονται σε όλη την διάρκεια των σπουδών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Καρούμπαλης Ευθύμιος (2010), Διπλωματική εργασία με θέμα “Πληροφοριακά συστήματα στην διοίκηση και η χρήση τους σε ελληνική επιχείρηση”, Τμήματος Πληροφορικής, Πανεπιστημίου Πειραιώς
2. Δημήτρης Αρ. Γκριτζαλής, Διδακτορική διατριβή με θέμα “Ασφάλεια πληροφοριακών συστημάτων σε περιβάλλοντα υψηλής ευπάθειας” του Τμήματος Μαθηματικών, Πανεπιστήμιο Αιγαίου.
3. Γ. Πάγκαλος-Ι. Μαυρίδης (2002), Σύγγραμμα Έυδοξου με τίτλο “Βασικές θέματα ασφάλειας πληροφοριακών συστημάτων και επικοινωνία” αποσπάσματα από το σύγγραμμα [chapter-5425.pdf \(eudoxus.gr\)](#)
4. Επιστήμης Υπολογιστών (Ηράκλειο) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

Links:

<https://www.uoc.gr>

<http://www.csd.uoc.gr/~hy457>

https://www.csd.uoc.gr/CSD/index.jsp?content=courses_catalog&openmenu=demoAcc3&lang=gr

5. Εφαρμοσμένης Πληροφορικής - Πληροφοριακά Συστήματα (Θεσσαλονίκη) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

Links: <https://www.uom.gr/idrymatikos-katalogos-mathimaton>

6. Πληροφορικής (Θεσσαλονίκη) - ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

Links: <https://elearning.auth.gr> <https://www.csd.auth.gr>

7. Πληροφορικής (Κέρκυρα) - ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Links: [ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ | Πρόγραμμα Σπουδών \(ionio.gr\)](#)

8. Εφαρμοσμένης Πληροφορικής - Πληροφοριακά Συστήματα (Θεσσαλονίκη) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

Links: <https://www.uom.gr/idrymatikos-katalogos-mathimaton>

9. Πληροφορικής (Αθήνα) - ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
Links: <https://www.aueb.gr>
10. Πληροφορικής (Πειραιάς) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
Links: <https://www.unipi.gr/unipi/el/plh-home.html>
11. Πληροφορικής και Τηλεματικής (Αθήνα) - ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
Links: <https://www.dit.hua.gr/index.php/el>
12. Πληροφορικής και Τηλεπικοινωνιών (Τρίπολη) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
Links: <https://dit.uop.gr/index.php/el>
13. Πληροφορικής και Τηλεπικοινωνιών (Λαμία) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
Links: <https://dit.uth.gr>
14. Πληροφορικής με Εφαρμογές στη Βιοϊατρική (Λαμία) - ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
Links: <https://dib.uth.gr>
15. Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής (Ιωάννινα)- Πολυτεχνική Σχολή - Πανεπιστήμιο Ιωαννίνων
Links: [Computer Science and Engineering Department – Πανεπιστήμιο Ιωαννίνων \(uoi.gr\)](#)
16. Μηχανικών Ηλεκτρονικών υπολογιστών και Πληροφορικής (Πάτρα)- Πανεπιστήμιο Πατρών
Links: [Τμήμα Μηχανικών Η/Υ & Πληροφορικής | Πανεπιστήμιο Πατρών \(upatras.gr\)](#)
17. Μηχανικών Πληροφοριακών Επικοινωνιών και Συστημάτων (Αιγαίο)- Πολυτεχνικής Σχολής του Πανεπιστημίου Αιγαίου-
Link: [Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων \(aegean.gr\)](#)
18. Χαροκοπείο πανεπιστήμιο - Σχολή πληροφορικής και Τηλεματικής
Links: [Πληροφορίες \(hua.gr\)](#)
19. Ιστοσελίδα με την παροχή όλων των Πανεπιστημίων και Πολυτεχνικών Σχολών
Links: <https://aeitei.gr/omades.php?omada=692>
<https://aeitei.gr/omades.php?omada=673>

