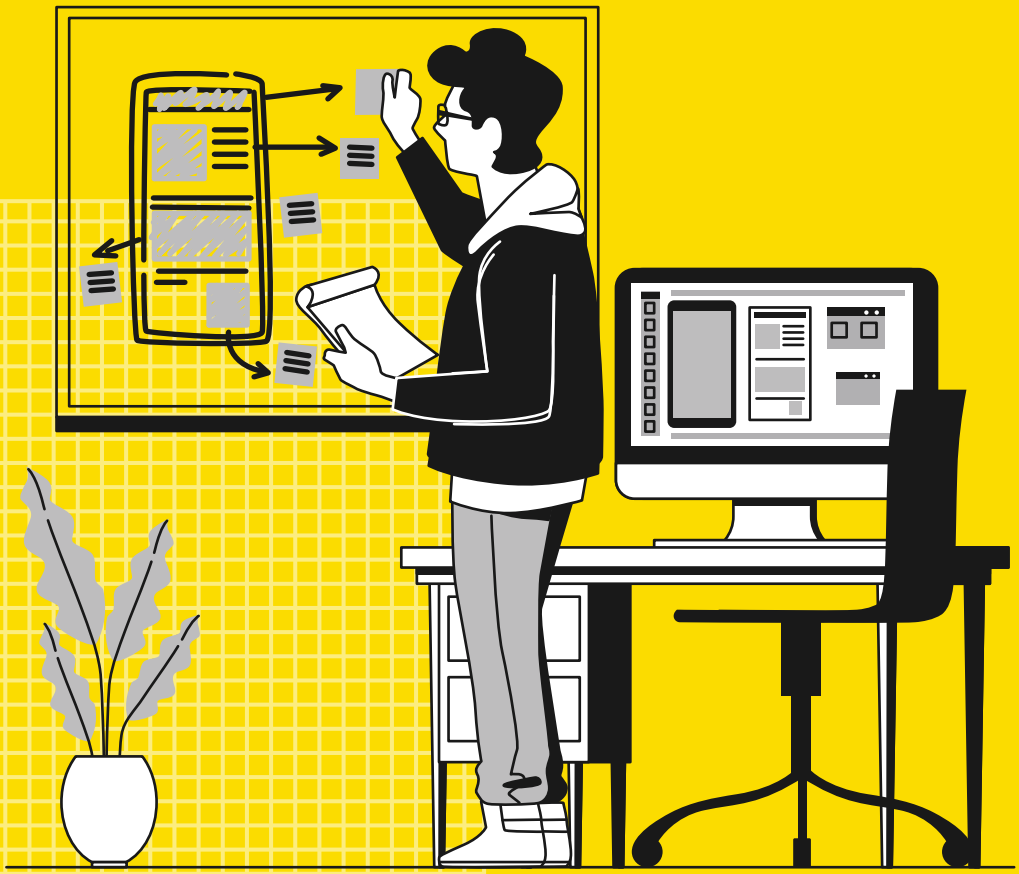
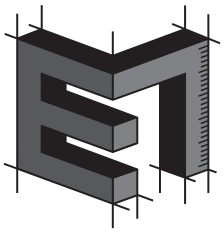
ΕΟΠΠΕΠ
ΕΘΝΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΠΡΟΣΟΝΤΩΝ & ΕΠΑΓΓΕΛΜΑΤΙΚΟΥ ΠΡΟΣΑΝΑΤΟΛΙΣΜΟΥ

ΕΠΑΓΓΕΛΜΑΤΙΚΟ
ΠΕΡΙΓΡΑΜΜΑ

# Τεχνικός ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist)





ΕΠΑΓΓΕΛΜΑΤΙΚΟ
ΠΕΡΙΓΡΑΜΜΑ

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2021-2027
Βιώσιμη Ανάπτυξη για Όλους

Πρόγραμμα
Ανθρώπινο Δυναμικό και Κοινωνική Συνοχή

ΕΠΑΓΓΕΛΜΑΤΙΚΟ
ΠΕΡΙΓΡΑΜΜΑ

# Τεχνικός ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist)

| Εκδόσεις | | | | |
|---|---|---|---|---|
| Περιγραφή | Έτος | Φορέας συντονισμού ομάδας εκπόνησης | Συνεργαζόμενος φορέας | Ομάδα εκπόνησης ΕΠ |
| Πρώτη έκδοση | 2023 | ΣΕΒ/ΣΤΕΓΗ | ΓΣΕΕ | • Αναστάσιος Παπαθανασίου<br>• Άννα Γιαννούτσου<br>• Γεώργιος Μπαγλατζής<br>• Χρήστος Κούκιος<br>• Νικόλαος Σάμιος<br>• Χριστίνα Παππά<br>• Ντόρα Οικονόμου<br>• Τέσσα Μίχου<br>• Νίκος Γαβαλάκης<br>• Ελευθερία Ρώμα<br>• Ζήσης Μανούζας |

Το παρόν Επαγγελματικό Περίγραμμα πιστοποιήθηκε
με την υπ΄αριθ. πρωτ.: 50229 / 8-11-2024 Απόφαση
της 602ης/7-11-2024 Συνεδρίασης του Δ.Σ. του Ε.Ο.Π.Π.Ε.Π.

**Συγγραφέας**
Αναστάσιος Παπαθανασίου

**Εμπειρογνώμονες επαγγέλματος**
Άννα Γιαννούτσου
Γεώργιος Μπαγλατζής

**Εμπειρογνώμονας εκπρόσωπος συνεργαζόμενης αντιπροσωπευτικής οργάνωσης εργοδοτών (ΣΕΒ)**
Χρήστος Κούκιος

**Εμπειρογνώμονας εκπρόσωπος συνεργαζόμενης αντιπροσωπευτικής οργάνωσης εργαζομένων (ΓΣΕΕ)**
Νικόλαος Σάμιος

**Σύμβουλος Επαγγελματικού Περιγράμματος**
Χριστίνα Παππά

Το περιεχόμενο της παρούσας μελέτης διαμορφώθηκε από ομάδα εκπόνησης υπό την εποπτεία της Ανώνυμης Εταιρείας Αναπτυξιακών Δράσεων Στέγη της Ελληνικής Βιομηχανίας, με βάση μεθοδολογικές προδιαγραφές και ειδικά πρότυπα που αναπτύχθηκαν από τα Ινστιτούτα ΙΝΕ ΓΣΕΕ και ΙΜΕ ΓΣΕΒΕΕ και εγκρίθηκαν από τον Ε.Ο.Π.Π.Ε.Π., στο πλαίσιο της Πράξης «Ανάπτυξη, Επικαιροποίηση και Πιστοποίηση Επαγγελματικών Περιγραμμάτων και Πλαισίων Εκπαιδευτικών Προδιαγραφών Προγραμμάτων» με κωδικό ΟΠΣ (MIS) 5075008 στο Επιχειρησιακό Πρόγραμμα «Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση».

Η Πράξη υλοποιήθηκε με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης (Ευρωπαϊκό Κοινωνικό Ταμείο – Ε.Κ.Τ.).

Οι συμπράττοντες φορείς που σχεδίασαν και υλοποίησαν την Πράξη είναι:

(α) Τα επιστημονικά Ινστιτούτα των κοινωνικών εταίρων ΓΣΕΕ, ΣΕΒ, ΓΣΕΒΕΕ, ΕΣΕΕ, ΣΕΤΕ:

- Ινστιτούτο Εργασίας Γενικής Συνομοσπονδίας Εργατών Ελλάδος (ΙΝΕ ΓΣΕΕ),
- Ανώνυμη Εταιρεία Αναπτυξιακών Δράσεων Στέγη της Ελληνικής Βιομηχανίας,
- Ινστιτούτο Μικρών Επιχειρήσεων Γενικής Συνομοσπονδίας Επαγγελματιών Βιοτεχνών Εμπόρων Ελλάδας (ΙΜΕ ΓΣΕΒΕΕ)
- Κέντρο Ανάπτυξης Ελληνικού Εμπορίου και Επιχειρηματικότητας της Ελληνικής Συνομοσπονδίας Εμπορίου και Επιχειρηματικότητας (ΚΑΕΛΕ ΕΣΕΕ),
- Ινστιτούτο Συνδέσμου Ελληνικών Τουριστικών Επιχειρήσεων (ΙΝΣΕΤΕ) και

(β) ο Εθνικός Οργανισμός Πιστοποίησης Προσόντων & Επαγγελματικού Προσανατολισμού (Ε.Ο.Π.Π.Ε.Π.).

Συντονιστής φορέας της σύμπραξης ήταν το ΙΜΕ ΓΣΕΒΕΕ.

Ομάδα διοίκησης και διαχείρισης του έργου αποτέλεσαν οι:

- Παρασκευάς Λιντζέρης (Υπεύθυνος Πράξης), Γεωργία Μιχαλοπούλου, Κωνσταντίνα Λουλούδη (ΙΜΕ ΓΣΕΒΕΕ - συντονιστής σύμπραξης),
- Δήμητρα Δέδε, Μαρίνα Κατσιμάνη (Ε.Ο.Π.Π.Ε.Π.),
- Χρήστος Γούλας, Ρένα Βαρβιτσιώτη, Ιάκωβος Καρατράσογλου, Παναγιώτης Νάτσης (ΙΝΕ ΓΣΕΕ),
- Τέσσα Μίχου, Χριστίνα Παππά, Ελευθερία Ρώμα (ΣΤΕΓΗ της ΕΛΛΗΝΙΚΗΣ ΒΙΟΜΗΧΑΝΙΑΣ),
- Δημήτρης Πρίφτης, Χρήστος Συρομάχος, Μαρία Περγιουδάκη, Δέσποινα Ρέππα, Πηνελόπη Γιαννακοπούλου (ΚΑΕΛΕ ΕΣΕΕ),
- Μιχάλης Κυριακίδης, Γιώργος Δαλκίδης, Αναστασία Αντωνοπούλου (ΙΝΣΕΤΕ).

# Περιεχόμενα

## ΠΕΡΙΛΗΨΗ

Η παρούσα μελέτη αφορά στο επαγγελματικό περίγραμμα του/της «Τεχνικού ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist)», ο/η οποίος/α ασχολείται με το σχεδιασμό, εφαρμογή, παρακολούθηση και έλεγχο της εφαρμογής των μέτρων ασφάλειας πληροφοριακών συστημάτων και δικτύων σε έναν Οργανισμό, προκειμένου να επιτευχθούν οι ακόλουθοι στόχοι της ασφάλειας πληροφοριών: εμπιστευτικότητα (confidentiality), ακεραιότητα (integrity) και διαθεσιμότητα (availability) των πληροφοριών/δεδομένων του Οργανισμού. Επίσης ενημερώνει, συμβουλεύει και υποστηρίζει τους χρήστες των πληροφοριακών συστημάτων και τη Διοίκηση του Οργανισμού σε θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων.

Οι προοπτικές απασχόλησης, ως Τεχνικός ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist), είναι αρκετά θετικές σε διάφορους τομείς και τύπους οργανισμών και επιχειρήσεων, όπου υπάρχουν και χρησιμοποιούνται υπολογιστικά και πληροφοριακά συστήματα και αναμένεται να παρουσιάσουν σημαντική ανάπτυξη στο μέλλον, λόγω της ανάγκης για αυξημένη ασφάλεια και προστασία των πληροφοριακών συστημάτων, δικτύων και πληροφοριών/δεδομένων κάθε οργανισμού και επιχείρησης, ένεκα των αυξανόμενων κυβερνοαπειλών και κυβερνοεπιθέσεων.

Το παρόν επαγγελματικό περίγραμμα του/της «Τεχνικού ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist)» οριοθετεί τις γνώσεις, δεξιότητες και ικανότητες που απαιτούνται για την άσκηση του επαγγέλματος και αναλύει τις κεντρικές επαγγελματικές λειτουργίες, ώστε να είναι σαφώς προσδιορισμένες οι επιμέρους επαγγελματικές λειτουργίες και οι παρεχόμενες υπηρεσίες, καθώς και οι διαδρομές απόκτησης των απαιτούμενων γνώσεων, δεξιοτήτων και ικανοτήτων.

## ABSTRACT

The present study concerns the occupational profile of the "IT Security Technician/Specialist ", who deals with the design, implementation and monitoring of Information System and network security measures in an organization, in order to achieve the following objectives of information security: confidentiality, integrity and availability of information/data of the organization. It also informs, advises, and supports the users of Information Systems and the administration of the organization on information security and data protection issues.

The employment prospects as an IT security Technician/Specialist are truly positive in various sectors and types of organizations and businesses where computer and information systems are used and are expected to show significant growth in the future, due to the need for increased security and protection of information systems, networks and information/data of each organization and business, due to the increasing cyber threats and cyberattacks.

The occupational profile outlines the knowledge, skills and competences required for the profession of the “IT Security Technician/Specialist” and analyzes the central professional functions, so that the specific professional functions and services provided are clearly defined, as well as the paths of obtaining the required knowledge, skills and abilities.

# ΕΙΣΑΓΩΓΗ[1]

Η παρούσα μελέτη περιλαμβάνει το επαγγελματικό περίγραμμα και το πλαίσιο εκπαιδευτικών προδιαγραφών προγραμμάτων επαγγελματικής εκπαίδευσης και κατάρτισης για το επάγγελμα του/της «Τεχνικού ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist)».

Το επαγγελματικό περίγραμμα συνιστά μια κωδικοποιημένη αποτύπωση του περιεχομένου του επαγγέλματος, καθώς και των απαιτούμενων για την άσκησή του προσόντων, όπως ορίζονται στην υπ΄ αριθμ. 110988 ΚΥΑ (ΦΕΚ 566/8.5.06) με περιεχόμενο «Πιστοποίηση Επαγγελματικών Περιγραμμάτων». Αντίστοιχα, το πλαίσιο εκπαιδευτικών προδιαγραφών προγραμμάτων επαγγελματικής εκπαίδευσης και κατάρτισης αξιοποιεί στο ακέραιο την «πρώτη ύλη» του επαγγελματικού περιγράμματος και διατυπώνει τις ελάχιστες βασικές προδιαγραφές που προηγούνται του κάθε εκπαιδευτικού σχεδιασμού, ανεξάρτητα από τα ιδιαίτερα θεσμικά του χαρακτηριστικά.

Η δομή, το περιεχόμενο και ο τρόπος παρουσίασης της μελέτης, δίνει τη δυνατότητα αξιοποίησής της από πολλαπλές ομάδες απεύθυνσης, εξυπηρετώντας διαφορετικούς κάθε φορά σκοπούς.

Ειδικότερα, μπορεί να αξιοποιηθεί από:

- εργαζόμενους ή ανέργους, ως εργαλείο πληροφόρησης για το επάγγελμα ή περιγραφής και τεκμηρίωσης των γνώσεων/δεξιοτήτων/ικανοτήτων τους,
- υπηρεσίες απασχόλησης και συμβουλευτικής σταδιοδρομίας, κατά τη παροχή των υπηρεσιών τους
- φορείς εκπαίδευσης/κατάρτισης, για να προσαρμόσουν τα προγράμματά τους,
- επιχειρήσεις, για να περιγράψουν με μεγαλύτερη ακρίβεια τις δεξιότητες και τα προσόντα των εργαζομένων στις σχετικές θέσεις εργασίας.

Η μελέτη ακολουθεί ένα δομημένο πρότυπο με συγκεκριμένες μεθοδολογικές προδιαγραφές που ορίζονται στις *Προδιαγραφές Εκσυγχρονισμένης Μεθοδολογίας, Προτύπων και Εργαλείων Εκπόνησης Επαγγελματικών Περιγραμμάτων και Πλαισίων Προδιαγραφών Προγραμμάτων*[2]*, οι οποίες* εγκρίθηκαν με την υπ' αριθμ. ΓΔ/12832/15-04-21 Απόφαση της υπ' αριθμ. 443ης/14-04-21 Συνεδρίασης του Δ.Σ. του Ε.Ο.Π.Π.Ε.Π.

Συγκεκριμένα, η μελέτη εμπεριέχει: i) την εισαγωγή, ii) τη σύνοψη του επαγγελματικού περιγράμματος, iii) την ανάλυση του επαγγελματικού περιγράμματος, iv) τη βιβλιογραφία και v) το Πλαίσιο Εκπαιδευτικών Προδιαγραφών Προγραμμάτων.

i) Η **εισαγωγή** προσδιορίζει αδρά το περιεχόμενο της μελέτης και τον τρόπο αξιοποίησής της.

ii) Η **σύνοψη** του επαγγελματικού περιγράμματος, παρουσιάζει περιληπτικά τις βασικές πληροφορίες της ανάλυσης του επαγγέλματος.

iii) Η **ανάλυση του επαγγελματικού περιγράμματος** περιλαμβάνει τις παρακάτω ενότητες:

- Ενότητα **Α**: Τίτλος και ορισμός του επαγγέλματος / ειδικότητας.
- Ενότητα **Β**: Ανάλυση του επαγγέλματος / ειδικότητας – «προδιαγραφές».

[1] Όπου στο κείμενο του επαγγελματικού περιγράμματος αναφέρεται ο όρος «Ινστιτούτα Επαγγελματικής Κατάρτισης» ή το αρκτικόλεξο «Ι.Ε.Κ.», νοούνται οι Σχολές Ανώτερης Επαγγελματικής Κατάρτισης ή το αρκτικόλεξο «Σ.Α.Ε.Κ.», αντίστοιχα. Σχετ. παρ.2, άρθρο 3 του ν. 5082/2024 (Α'9)

[2] Καραλής, Θ., Μαρκίδης, Κ., Βαρβιτσιώτη, Ρ., Νάτσης, Π., Καρατράσογλου, Ι., Παπαευσταθίου, Κ., Γούλας, Χ., & Λιντζέρης, Π. (2021) *Μεθοδολογικές προσεγγίσεις ανάπτυξης επαγγελματικών περιγραμμάτων και πλαισίων εκπαιδευτικών προδιαγραφών προγραμμάτων,* Αθήνα: ΙΝΕ ΓΣΕΕ.

- Ενότητα Γ: Απαραίτητες γνώσεις, δεξιότητες και ικανότητες για την άσκηση του επαγγέλματος/ ειδικότητας.
- Ενότητα Δ: Προτεινόμενες διαδρομές για την απόκτηση των απαιτούμενων προσόντων.
- Ενότητα Ε: Ενδεικτικοί τρόποι αξιολόγησης των απαιτούμενων γνώσεων, δεξιοτήτων και ικανοτήτων.

Στην Ενότητα Α καταγράφονται οι γενικότερες συνθήκες άσκησης του επαγγέλματος, οι τεχνολογικές και άλλες αλλαγές που το επηρεάζουν, οι προοπτικές του επαγγέλματος στην αγορά εργασίας και των κλάδων δραστηριότητας στους οποίους ασκείται, καθώς και οι ρυθμίσεις που ισχύουν σχετικά με την άσκησή του.

Στην Ενότητα Β αποτυπώνεται το περιεχόμενο του επαγγέλματος. Αναλύεται σε Κύριες Επαγγελματικές Λειτουργίες ($ΚΕΛ_1$ έως $ΚΕΛ_ν$), κάθε ΚΕΛ αναλύεται σε Επιμέρους Επαγγελματικές Λειτουργίες (ΕΕΛ) και κάθε ΕΕΛ σε Επαγγελματικές Εργασίες (ΕΕ). Για κάθε ΕΕΛ προσδιορίζονται τα Κριτήρια Επαγγελματικής Ανταπόκρισης (ΚΕΑ) και το Εύρος Εφαρμογής (ΕυΕ) της.

Στην Ενότητα Γ αναλύονται οι απαιτούμενες γνώσεις, δεξιότητες και ικανότητες που είναι απαραίτητες για την αποτελεσματική εκτέλεση κάθε ΕΕΛ.

Στην Ενότητα Δ καταγράφονται οι διαδρομές για την απόκτηση των απαιτούμενων προσόντων.

Στην Ενότητα Ε οι ενδεικτικοί τρόποι αξιολόγησης των απαιτούμενων γνώσεων και δεξιοτήτων.

iv) Στη βιβλιογραφία παρατίθενται βιβλία, άρθρα κ.λπ. πάνω στα οποία στηρίζεται η συγγραφή των ενοτήτων του επαγγελματικού περιγράμματος ενώ, παράλληλα, συνιστούν προτάσεις για περαιτέρω μελέτη και εμβάθυνση στο αντικείμενο ή στο επάγγελμα.

Για την ανάπτυξη της παρούσας μελέτης συστάθηκε ομάδα εργασίας στην οποία συμμετείχαν ο κος Αναστάσιος Παπαθανασίου (συγγραφέας), ο κος Χρήστος Κούκιος (εμπειρογνώμονας-εκπρόσωπος αντιπροσωπευτικής οργάνωσης εργοδοτών, εν προκειμένω του ΣΕΒ), ο κος Νικόλαος Σάμιος ((εμπειρογνώμονας-εκπρόσωπος αντιπροσωπευτικής οργάνωσης εργαζομένων, εν προκειμένω της ΓΣΕΕ), η κα Άννα Γιαννούτσου και ο κος Γεώργιος Μπαγλατζής (εμπειρογνώμονες επαγγέλματος) και η κα Χριστίνα Παππά (σύμβουλος επαγγελματικού περιγράμματος).

Η τελική σύνθεση του Επαγγελματικού Περιγράμματος πραγματοποιήθηκε από τον συγγραφέα, με την υποστήριξη των επιστημονικών στελεχών του ΣΕΒ/ΣΤΕΓΗ κ.κ. Τέσσας Μίχου, Νίκου Γαβαλάκη, Ελευθερίας Ρώμα και Ζήση Μανούζα, υπό την επιστημονική εποπτεία της Διευθύντριας Τομέα Ανάπτυξης Ανθρώπινου Δυναμικού του ΣΕΒ, κας Ντόρας Οικονόμου.

**ΣΥΝΟΨΗ**

# Τεχνικός ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist)[3]

## ΠΕΡΙΓΡΑΦΗ ΕΠΑΓΓΕΛΜΑΤΟΣ

Ο Τεχνικός ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist) ασχολείται με το σχεδιασμό, εφαρμογή, παρακολούθηση και έλεγχο της εφαρμογής των μέτρων ασφάλειας πληροφοριακών συστημάτων και δικτύων σε έναν Οργανισμό, προκειμένου να επιτευχθούν οι ακόλουθοι στόχοι της ασφάλειας πληροφοριών: εμπιστευτικότητα (confidentiality), ακεραιότητα (integrity) και διαθεσιμότητα (availability) των πληροφοριών/δεδομένων του Οργανισμού. Επίσης ενημερώνει, συμβουλεύει και υποστηρίζει τους χρήστες των πληροφοριακών συστημάτων και τη Διοίκηση του Οργανισμού σε θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων.

## ΠΕΡΙΒΑΛΛΟΝ ΕΝΑΣΧΟΛΗΣΗΣ

- Επιχειρήσεις, Οργανισμοί, Υπηρεσίες κλπ., όπου υπάρχουν και χρησιμοποιούνται υπολογιστικά και πληροφοριακά συστήματα, καθώς και δικτυακός εξοπλισμός,
- Επιχειρήσεις και Οργανισμοί, που κατασκευάζουν, προωθούν - πωλούν και υποστηρίζουν προϊόντα ή υπηρεσίες Πληροφορικής,
- Εμπορικές αντιπροσωπείες προϊόντων υπολογιστικών συστημάτων,
- Επιχειρήσεις που παρέχουν υπηρεσίες υποστήριξης και συμβουλευτικής προς τρίτους ή/και παροχή συμβουλευτικών υπηρεσιών σε θέματα IT Security, Cyber security και Security as a service κτλ.

## ΠΡΟΫΠΟΘΕΣΕΙΣ ΑΣΚΗΣΗΣ ΕΠΑΓΓΕΛΜΑΤΟΣ

Δεν απαιτείται άδεια ασκήσεως επαγγέλματος, ούτε υπάρχουν άλλες προϋποθέσεις για την άσκηση του επαγγέλματος.

## ΥΦΙΣΤΑΜΕΝΕΣ ΚΑΙ ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΔΙΑΔΡΟΜΕΣ ΑΠΟΚΤΗΣΗΣ ΤΩΝ ΑΠΑΙΤΟΥΜΕΝΩΝ ΠΡΟΣΟΝΤΩΝ

| ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΔΙΑΔΡΟΜΕΣ | |
|---|---|
| 1η Διαδρομή | Δίπλωμα Ινστιτούτου Επαγγελματικής Κατάρτισης (ΙΕΚ) επιπέδου 5 του ΕΠΠ στις ειδικότητες του Τομέα Πληροφορικής – Συνεχιζόμενη επαγγελματική κατάρτιση για το σύνολο των γνώσεων που αντιστοιχούν στις 2 Κύριες Επαγγελματικές Λειτουργίες του επαγγέλματος (ΚΕΛ 1, ΚΕΛ 2) |
| 2η Διαδρομή | Δίπλωμα Μεταλυκειακού Έτους-Τάξης Μαθητείας επιπέδου 5 του ΕΠΠ στις ειδικότητες του τομέα Πληροφορικής (Τεχνικός Εφαρμογών Πληροφορικής ή Τεχνικός Η/Υ και Δικτύων Η/Υ) – Συνεχιζόμενη επαγγελματική κατάρτιση για το σύνολο των γνώσεων που αντιστοιχούν στις 2 Κύριες Επαγγελματικές Λειτουργίες του επαγγέλματος (ΚΕΛ 1, ΚΕΛ 2) |
| 3η Διαδρομή | Πτυχίο Επαγγελματικού Λυκείου (ΕΠΑ.Λ.) επιπέδου 4 του ΕΠΠ στις ειδικότητες του τομέα Πληροφορικής (Τεχνικός Εφαρμογών Πληροφορικής ή Τεχνικός Η/Υ και Δικτύων Η/Υ) – 1 έτος συναφής επαγγελματική εμπειρία – Συνεχιζόμενη επαγγελματική κατάρτιση για το σύνολο των γνώσεων που αντιστοιχούν στις 2 Κύριες Επαγγελματικές Λειτουργίες του επαγγέλματος (ΚΕΛ 1, ΚΕΛ 2) |

[3]Στην παρούσα μελέτη η φράση «Τεχνικός ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist» αναφέρεται και στα δύο φύλα. Το αρσενικό γραμματικό γένος χρησιμοποιείται για καθαρά πρακτικούς λόγους.

| | |
|---|---|
| 4η Διαδρομή | Πτυχίο Επαγγελματικής Σχολής (ΕΠΑ.Σ.) Μαθητείας της ΔΥΠΑ επιπέδου 3 του ΕΠΠ της ειδικότητας «Τεχνίτης Υποστήριξης Συστημάτων Υπολογιστών» – 1,5 έτος συναφής επαγγελματική εμπειρία – Συνεχιζόμενη επαγγελματική κατάρτιση για το σύνολο των γνώσεων που αντιστοιχούν στις 2 Κύριες Επαγγελματικές Λειτουργίες του επαγγέλματος (ΚΕΛ 1, ΚΕΛ 2) |
| 5η Διαδρομή | Απόφοιτοι Δευτεροβάθμιας Εκπαίδευσης (Γενικού Λυκείου) επιπέδου 4 του ΕΠΠ – 2 έτη συναφής επαγγελματική εμπειρία – Συνεχιζόμενη επαγγελματική κατάρτιση για το σύνολο των γνώσεων που αντιστοιχούν στις 2 Κύριες Επαγγελματικές Λειτουργίες του επαγγέλματος (ΚΕΛ 1, ΚΕΛ 2) |

## ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΟΡΓΑΝΩΣΕΙΣ

- Ελληνική Εταιρεία Επιστημόνων και Επαγγελματιών Πληροφορικής και Επικοινωνιών (ΕΠΥ - http://www.epy.gr)
- Ένωση Πληροφορικών Ελλάδος (ΕΠΕ - https://www.epe.org.gr)
- Ελληνικό Δίκτυο Επαγγελματιών Πληροφορικής (HEPIS - https://www.hepis.gr)
- Οργανισμός Ανοιχτών Τεχνολογιών (ΕΕΛΛΑΚ - https://eellak.ellak.gr/)
- Ένωση Μηχανικών Πληροφορικής και Επικοινωνιών Ελλάδας (ΕΜηΠΕΕ - https://www.computer-engineers.gr)
- Ελληνική Επιστημονική Ένωση Τεχνολογιών Πληροφορίας & Επικοινωνιών στην Εκπαίδευση (ΕΤΠΕ - https://www.etpe.gr)
- Πανελλήνια Ένωση Καθηγητών Πληροφορικής Δευτεροβάθμιας Εκπαίδευσης (Π.Ε.ΚΑ.Π. - http://www.pekap.gr)
- Τεχνικό Επιμελητήριο Ελλάδας (ΤΕΕ - https://web.tee.gr), Τμήμα Ηλεκτρολόγων/Ηλεκτρονικών Μηχανικών και Πληροφορικής.
- Σύνδεσμος Επιχειρήσεων Πληροφορικής & Επικοινωνιών Ελλάδας (ΣΕΠΕ - http://www.sepe.gr)
- Σύνδεσμος Επιχειρήσεων Πληροφορικής Βορείου Ελλάδος (ΣΕΠΒΕ - http://www.sepve.org)
- Council of European Professional Informatics Societies (CEPIS - http://www.cepis.org)
- Computer & Communications Industry Association (CCIA - https://www.ccianet.org)
- European e-Skills Association (EeSA - http://eskillsassociation.eu)
- UNI Europa - European services workers union (http://www.uni-europa.org)

## ΑΡΜΟΔΙΟΤΗΤΕΣ

- Σχεδιάζει τα μέτρα ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού
- Εφαρμόζει τα μέτρα ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού
- Ελέγχει τα μέτρα ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού
- Ενημερώνει τους χρήστες των πληροφοριακών συστημάτων και τη Διοίκηση του Οργανισμού για θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων
- Υποστηρίζει τους χρήστες των πληροφοριακών συστημάτων και τη Διοίκηση του Οργανισμού για θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων.

## ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΓΝΩΣΕΙΣ

- Αλγόριθμοι, πρωτόκολλα και λογισμικά κρυπτογράφησης και αποκρυπτογράφησης, ψευδωνυμοποίησης και ανωνυμοποίησης
- Αρχές συντήρησης και αναβάθμισης υλικού και λογισμικού
- Ασφάλεια πληροφοριακών συστημάτων, δικτύων και πληροφοριών
- Βασικές γνώσεις, έννοιες και εντολές προγραμματισμού Η/Υ
- Γνώσεις διασύνδεσης, συνδεσμολογίας και αρχιτεκτονικής δικτύων και υπολογιστικών συστημάτων
- Γνώσεις εντοπισμού και εφαρμογής ενημερώσεων και ελάχιστων προδιαγραφών ασφάλειας υπολογιστικών συστημάτων, λογισμικών και εφαρμογών
- Γνώση και υλοποίηση προτύπων ασφάλειας πληροφοριών (όπως, ISO/IEC 27001, 27002, ISO/IEC 29151, Control Objectives for Information Technology (CobIT), Common Criteria, NIST/SP 800-53, ENISA)
- Γνώση τεχνολογιών και λογισμικών που ανιχνεύουν την εγκατάσταση, εκτέλεση και μετάδοση κακόβουλου/ιομορφικού λογισμικού
- Γνώσεις για τεχνικούς ελέγχους αξιολόγησης (Penetration tests, vulnerability assessment, security code reviews) της επάρκειας, καταλληλόλητας και αποτελεσματικότητας μέτρων ασφάλειας πληροφοριακών συστημάτων.
- Γνώσεις και εργαλεία για διενέργεια πρακτικών ασκήσεων προσομοίωσης συμβάντων και περιστατικών ασφάλειας
- Γνώσεις αντιμετώπισης κυβερνοεπιθέσεων
- Διαδικασίες, τεχνικές, εργαλεία και μεθοδολογίες ελέγχου ασφάλειας πληροφορικών συστημάτων (IT Security Audit)
- Νομοθετικό και κανονιστικό πλαίσιο που σχετίζεται με την ασφάλεια πληροφοριακών συστημάτων, την προστασία προσωπικών δεδομένων και τη νομοθεσία περί προστασίας δικαιωμάτων χρήσης λογισμικού

- Πρωτόκολλα, τεχνολογίες και μηχανισμοί ταυτοποίησης και αυθεντικοποίησης
- Τεχνικές/διαδικασίες/πλατφόρμες εκπαίδευσης, ενημέρωσης και ευαισθητοποίησης υπαλλήλων/εργαζομένων σε βασικά θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων
- Τεχνική ορολογία (ελληνική και αγγλική).

## ΔΕΞΙΟΤΗΤΕΣ

- Αρχειοθέτηση νομοθετικών κειμένων, κανονισμών σε θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων
- Διαμόρφωση υλικού ενημέρωσης (σεμινάρια, φυλλάδια, γραπτά μηνύματα κτλ.)
- Εφαρμογή και χρήση προτύπων, κανόνων και εργαλείων σύγχρονης και ασύγχρονης επικοινωνίας.
- Εφαρμογή εργαλείων πρόληψης ή αποτροπής απώλειας δεδομένων/πληροφοριών (DLP – Data Loss Prevention)
- Εφαρμογή λογισμικών/προγραμμάτων λήψης αντιγράφων ασφάλειας (backup)
- Εφαρμογή τεχνικών εκπαίδευσης ενηλίκων
- Εφαρμογή μέτρων αντιμετώπισης κυβερνοεπιθέσεων
- Κατάρτιση και συντήρηση καταλόγου-μητρώου (inventory) πληροφοριακών, επικοινωνιακών και δικτυακών υποδομών και συστημάτων.
- Συγγραφή, σχεδιασμός και ανάπτυξη πολιτικών, διαδικασιών τεχνικών και εγχειρίδιων ασφάλειας πληροφοριακών συστημάτων καθώς και κατάρτιση και προώθηση κατευθυντηρίων γραμμών.
- Τήρηση και εφαρμογή εθνικών και διεθνών προτύπων/τεχνικών/μεθοδολογιών ασφάλειας πληροφοριών και προστασίας των δεδομένων
- Χρήση προγραμμάτων, λογισμικών και λειτουργικών συστημάτων (προγράμματα εφαρμογών γραφείου, προγράμματα επεξεργασίας φωτογραφίας και εικόνων, προγράμματα διαχείρισης προσωπικών πληροφοριών, προγράμματα συμπίεσης/αποσυμπίεσης αρχείων, λογισμικά εφαρμογών, λογισμικά συστήματος, λειτουργικά συστήματα ανοικτού και κλειστού κώδικα κτλ.)
- Χρήση εργαλείων/μεθοδολογιών για διαχείριση, ανάλυση και αξιολόγηση κινδύνων (risk assessment), που σχετίζονται με τη λειτουργία και χρήση πληροφοριακών συστημάτων.
- Χρήση εργαλείων και τεχνολογιών για τη δημιουργία, εποπτεία και έλεγχο αντιγράφων ασφάλειας Χρήση εργαλείων για τεχνικούς ελέγχους ασφάλειας πληροφοριών.

## ΕΠΙΠΛΕΟΝ ΠΛΗΡΟΦΟΡΙΕΣ

- Εθνική Ακαδημία Ψηφιακών Ικανοτήτων - Gov.gr
  -https://nationaldigitalacademy.gov.gr/
- Udemy: Online Courses / Courses on Demand
  -https://www.udemy.com/
- Coursera Degrees, Certificates, & Free Online Courses
  -https://www.coursera.org/
- Κέντρο Ανοικτών Διαδικτυακών Μαθημάτων Mathesis
  -https://mathesis.cup.gr/
- edX Free Online Courses
  -https://www.edx.org/

ΕΝΟΤΗΤΑ Α

# ΤΙΤΛΟΣ ΚΑΙ ΟΡΙΣΜΟΣ ΕΠΑΓΓΕΛΜΑΤΟΣ

# ΕΝΟΤΗΤΑ Α: «Τίτλος και ορισμός του επαγγέλματος»

## Α.1 Προτεινόμενος γενικός τίτλος του επαγγέλματος

Ο τομέας των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) αναπτύχθηκε με ταχύτατους ρυθμούς τα τελευταία χρόνια και οι εφαρμογές και τα πληροφοριακά συστήματα χρησιμοποιούνται σε όλους τους κλάδους των καθημερινών δραστηριοτήτων της κοινωνίας και αγγίζουν κυριολεκτικά πλέον όλες τις πτυχές της καθημερινής μας ζωής.

Η αλματώδης αυτή ανάπτυξη των Τεχνολογιών Πληροφορικής και Επικοινωνιών, ανέδειξε παράλληλα την ανάγκη, για ενίσχυση της ασφάλειας και προστασίας των υπολογιστικών και πληροφοριακών συστημάτων από τις συνεχώς εξελισσόμενες ψηφιακές απειλές και τη δημιουργία ενός ξεχωριστού επαγγέλματος για το σκοπό αυτό, του Τεχνικού ασφάλειας συστημάτων πληροφορικής.

Ως εκ τούτου, η ομάδα ανάπτυξης του επαγγελματικού περιγράμματος προτείνει για το παρόν Επαγγελματικό Περίγραμμα τον τίτλο που έχει καθιερωθεί γενικότερα και στην αγορά εργασίας, ο οποίος είναι: Τεχνικός ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist).

## Α.2 Ορισμός του επαγγέλματος

Ο Τεχνικός ασφάλειας συστημάτων πληροφορικής σχεδιάζει, προτείνει, εφαρμόζει και παρακολουθεί τα μέτρα ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών σε έναν Οργανισμό, προκειμένου να επιτευχθούν οι ακόλουθοι στόχοι της ασφάλειας πληροφοριών: εμπιστευτικότητα (confidentiality), ακεραιότητα (integrity) και διαθεσιμότητα (availability) των πληροφοριών/δεδομένων του Οργανισμού. Επίσης ενημερώνει, συμβουλεύει και υποστηρίζει τους χρήστες των πληροφοριακών συστημάτων σε θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων.

Ειδικότερα, ο Τεχνικός ασφάλειας συστημάτων πληροφορικής έχει, στο πλαίσιο του κύριου αντικειμένου του, τις παρακάτω αρμοδιότητες, οι οποίες αναλύονται λεπτομερώς στις επόμενες ενότητες:

- Σχεδιάζει και προτείνει τα κατάλληλα μέτρα ασφάλειας των πληροφοριακών συστημάτων, των δικτύων και πληροφοριών σε έναν Οργανισμό.
- Εφαρμόζει και υλοποιεί τα κατάλληλα τεχνικά μέτρα ασφάλειας των πληροφοριακών συστημάτων, των δικτύων και των πληροφοριών σε έναν Οργανισμό.
- Επιβλέπει, παρακολουθεί και ελέγχει συστηματικά την τήρηση των μέτρων ασφάλειας των πληροφοριακών συστημάτων, των δικτύων και των πληροφοριών σε έναν Οργανισμό.
- Ενημερώνει, συμβουλεύει και ευαισθητοποιεί τους τελικούς χρήστες και τη Διοίκηση του Οργανισμού, σε θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων.
- Υποστηρίζει και καθοδηγεί τεχνικά τους χρήστες των πληροφοριακών συστημάτων σε θέματα ασφάλειας που ανακύπτουν και επιλύει τυχόν δυσλειτουργίες των πληροφοριακών συστημάτων, σχετιζόμενες με την ασφάλεια των συστημάτων πληροφορικής.

Ο Τεχνικός ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist) μπορεί να εργαστεί σε:

- Επιχειρήσεις, Οργανισμούς, Υπηρεσίες κλπ. όπου υπάρχουν και χρησιμοποιούνται υπολογιστικά και πληροφοριακά συστήματα, καθώς και δικτυακός εξοπλισμός.
- Επιχειρήσεις και Οργανισμούς, που κατασκευάζουν, προωθούν - πωλούν και υποστηρίζουν προϊόντα ή υπηρεσίες Πληροφορικής.
- Εμπορικές αντιπροσωπείες προϊόντων υπολογιστικών συστημάτων.
- Επιχειρήσεις που παρέχουν υπηρεσίες υποστήριξης και συμβουλευτικής προς τρίτους ή/και παροχή συμβουλευτικών υπηρεσιών σε θέματα IT Security, Cyber security και Security as a service κτλ.

Ο Τεχνικός ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist) λογοδοτεί απευθείας στο ανώτατο επίπεδο διοίκησης του Οργανισμού ή στον Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών, αν υφίσταται στον Οργανισμό, και δύναται να υποστηρίζεται στην άσκηση των καθηκόντων του

από ετέρους τεχνικούς-πληροφορικούς, με ειδίκευση είτε στις τεχνολογίες πληροφορικής και επικοινωνιών είτε στην ασφάλεια συστημάτων πληροφορικής.

## Α.3 Αντιστοίχιση με το ισχύον Σύστημα Ταξινόμησης Επαγγελμάτων και Κλάδων Οικονομίας.

Η αντιστοίχιση του επαγγέλματος του Τεχνικού ασφάλειας συστημάτων πληροφορικής όσον αφορά στην ταξινόμησή του σύμφωνα με το ισχύον Σύστημα Διεθνούς Τυποποιημένης Ταξινόμησης Επαγγελμάτων, βάσει ISCO 08 και σύμφωνα με το Σύστημα Στατιστικής Ταξινόμησης των Οικονομικών Δραστηριοτήτων (ΣΤΑΚΟΔ 08)[4], σε τετραψήφια ανάλυση, έχει ως εξής:

| | | |
|---|---|---|
| ISCO 08 | 3 | Τεχνικοί και ασκούντες συναφή επαγγέλματα |
| | 35 | Τεχνικοί του τομέα της πληροφόρησης και επικοινωνίας |
| | 351 | Τεχνικοί λειτουργιών και υποστήριξης χρηστών τεχνολογιών πληροφόρησης και επικοινωνίας |
| | 3512 | Τεχνικοί υποστήριξης χρηστών των τεχνολογιών πληροφόρησης και επικοινωνίας |
| | | |
| ΣΤΑΚΟΔ 08 | 62 | Δραστηριότητες προγραμματισμού ηλεκτρονικών υπολογιστών, παροχής συμβουλών και συναφείς δραστηριότητες |
| | 62.01 | Δραστηριότητες προγραμματισμού ηλεκτρονικών υπολογιστών, παροχής συμβουλών και συναφείς δραστηριότητες |
| | 62.09 | Άλλες δραστηριότητες της τεχνολογίας της πληροφορίας και δραστηριότητες υπηρεσιών ηλεκτρονικών υπολογιστών |

Πρέπει να τονιστεί ότι δεν υπάρχουν συγκεκριμένοι κωδικοί και στα δύο συστήματα ταξινόμησης που να ταυτίζονται πλήρως με τις δραστηριότητες του υπό εξέταση επαγγέλματος. Η αναφορά στους παραπάνω κωδικούς ΣΤΑΚΟΔ δεν είναι εξαντλητική και το επάγγελμά μπορεί να συναντηθεί και σε άλλους κλάδους, αλλά οι παραπάνω είναι οι κυριότεροι.

## Α.4 Ιστορική εξέλιξη του επαγγέλματος

Το επάγγελμα του Τεχνικού ασφάλειας συστημάτων πληροφορικής έχει αναπτυχθεί σταδιακά με την εξέλιξη της τεχνολογίας και την αυξανόμενη ανάγκη για ασφάλεια και προστασία των πληροφοριακών συστημάτων και δικτύων. Οι βασικές φάσεις ανάδυσης και εξέλιξης του επαγγέλματος και μια κωδικοποιημένη παρουσίαση των κύριων περιόδων, με αναφορά στις κομβικές αλλαγές που χαρακτήρισαν την εξέλιξή του, είναι οι ακόλουθες:

Αρχές-Μέσα της δεκαετίας 1980: Αρχές της Πληροφορικής και Ασφάλειας

Το πεδίο της ασφάλειας συστημάτων πληροφορικής ξεκίνησε να αναπτύσσεται στα τέλη της δεκαετίας του 1980. Το TCP/IP πρωτόκολλο δεν είχε καθιερωθεί ευρέως, οι υπολογιστικές μονάδες (Mainframe) βρίσκονταν κυρίως σε πανεπιστημιακά και ερευνητικά ιδρύματα, μεγάλους κρατικούς φορείς και ιδιωτικές εταιρείες, οι μεγάλοι κατασκευαστές (DEC, IBM, SUN) χρησιμοποιούσαν ιδιόκτητες σουίτες πρωτοκόλλων, όπως, το DECNET, IBM SNA κλπ., οι κύριες συνδέσεις ήταν με ασύγχρονα τερματικά και η ενασχόληση του τεχνικού ασφάλειας επικεντρωνόταν στην εφαρμογή και παρακολούθηση των κανόνων ασφαλούς χρήσης των πόρων των κεντρικών υπολογιστικών συστημάτων από τους χρήστες. Οι «πρώιμες» επιθέσεις αφορούσαν «εσωτερικές» επιθέσεις, με χρήση σχετικών συστημικών εντολών, προσπάθεια αναβάθμισης επιπέδου πρόσβασης και δημιουργία παράτυπου έως κακόβουλου κώδικα.

Δεκαετία 1990-2000: Αύξηση των διαδικτυακών απειλών

Με την εξάπλωση του διαδικτύου και την εμπορική του ευρείας κλίμακας χρήση, κατά τη δεκαετία του 1990, οι απειλές ασφάλειας έγιναν πιο εμφανείς, ενώ η ασφάλεια συστημάτων πληροφορικής έγινε ακόμη πιο σημαντική. Τα βασικά προβλήματα ασφάλειας περιλάμβαναν την ανεπάρκεια αυθεντικοποίησης, την αποκάλυψη

[4] Πηγή: https://www.statistics.gr/economic-activities

πληροφοριών και δεδομένων και τις επιθέσεις με κακόβουλο λογισμικό (malware), ενώ παράλληλα ξεκίνησε η ανάπτυξη εργαλείων και τεχνικών για την προστασία των συστημάτων πληροφορικής. Οι τεχνικοί ασφάλειας επικεντρώθηκαν στην ανάπτυξη αντιμετώπισης επιθέσεων και στην ανάλυση κινδύνων. Επιπλέον, άρχισαν να εμφανίζονται οι πρώτες πιστοποιήσεις ασφάλειας, που επιτρέπουν στους ειδικούς να επιδείξουν τις γνώσεις και τις δεξιότητές τους στον τομέα αυτό.

Δεκαετία 2000-2010: Επίθεση και άμυνα σε πραγματικό χρόνο

Κατά τη δεκαετία του 2000, οι επιθέσεις στα συστήματα πληροφορικής έγιναν πιο εξελιγμένες και η ικανότητα των επιτιθέμενων να προσβάλλουν τα συστήματα ήταν μεγαλύτερη. Αναπτύχθηκαν προηγμένες τεχνικές αποκάλυψης και προστασίας, καθώς και λύσεις ασφάλειας σε πραγματικό χρόνο.

Με την αύξηση των κυβερνοεπιθέσεων και των προηγμένων κινδύνων για την ασφάλεια των συστημάτων πληροφορικής, η ζήτηση για τεχνικούς ασφάλειας αυξήθηκε σημαντικά. Εμφανίστηκαν νέες τεχνικές επίθεσης και προηγμένα κακόβουλα λογισμικά, απαιτώντας συνεχή εκπαίδευση και εξειδίκευση για τους Τεχνικούς ασφάλειας, ενώ οι εταιρείες άρχισαν να συνειδητοποιούν τη σημασία της ασφάλειας και αυξήθηκε η ζήτηση για εξειδικευμένους Τεχνικούς ασφάλειας.

2010-σήμερα: Εξειδίκευση και αυξημένη πολυπλοκότητα

Η εξέλιξη της τεχνολογίας, τα μεγάλα περιστατικά παραβίασης και διαρροής δεδομένων και οι ολοένα αυξανόμενες απειλές ασφάλειας, οδήγησαν στο επίκεντρο ζητήματα που σχετίζονται με την ασφάλεια συστημάτων πληροφορικής.

Με την αύξηση της συνδεσιμότητας, των έξυπνων συσκευών και των υπηρεσιών υπολογιστικού νέφους (cloud computing), η ασφάλεια των συστημάτων πληροφορικής έχει γίνει πολυπλοκότερη. Οι τεχνικοί ασφάλειας πρέπει να εξειδικεύονται σε πολλούς τομείς, όπως η ανάλυση κινδύνων, η αποκάλυψη ευπαθειών, η ανάπτυξη ασφαλών λύσεων και η διαχείριση απειλών.

Ταυτόχρονα, οι επιθέσεις, χρησιμοποιώντας προηγμένες τεχνικές, όπως το ηλεκτρονικό ψάρεμα (phishing), το κακόβουλο λογισμικό/λυτρισμικό (ransomware) και η κοινωνική μηχανική (social engineering) έχουν αυξηθεί σημαντικά. Οι Τεχνικοί ασφάλειας πρέπει να παραμένουν ενημερωμένοι για τις τελευταίες τάσεις και τεχνολογίες ασφάλειας και να αναπτύσσουν συνεχώς νέες μεθόδους για την προστασία των συστημάτων, ενώ είναι πλέον απαραίτητοι για εταιρείες και οργανισμούς κάθε μεγέθους, προστατεύοντας τα δεδομένα τους, αντιμετωπίζοντας απειλές και προβλέποντας πιθανούς κινδύνους.

Επιπλέον, οι νομοθετικοί κανονισμοί για την προστασία των προσωπικών δεδομένων και την ασφάλεια πληροφοριών έχουν ενισχυθεί, όπως είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), αλλά και η οδηγία NIS και η νέα οδηγία NIS2 που ενισχύει τις απαιτήσεις κυβερνοασφάλειας που επιβάλλονται στις εταιρείες σε ένα διευρυμένο πεδίο, λαμβάνοντας υπόψη την ασφάλεια των αλυσίδων εφοδιασμού και τις σχέσεις με τους προμηθευτές. Όλοι αυτοί οι νέοι νομοθετικοί κανονισμοί απαιτούν από τις επιχειρήσεις και τους οργανισμούς να λάβουν αυξημένα μέτρα για την ασφάλεια και προστασία των πληροφοριακών συστημάτων και των προσωπικών δεδομένων των χρηστών.

Συνολικά, η εξέλιξη του επαγγέλματος του Τεχνικού ασφάλειας συστημάτων πληροφορικής αντικατοπτρίζει την αύξηση της σημασίας της ασφάλειας στον κυβερνοχώρο και την ανάγκη για εξειδικευμένους επαγγελματίες που θα προστατεύουν τα συστήματα και τις πληροφορίες από επιθέσεις.

Συνοψίζοντας, το επάγγελμα του Τεχνικού ασφάλειας συστημάτων πληροφορικής έχει αναπτυχθεί παράλληλα με την εξέλιξη της τεχνολογίας και την ανάγκη για προστασία των πληροφοριακών συστημάτων και δικτύων. Αρχικά, επικεντρωνόταν στην προστασία των υπολογιστών και των δικτύων, ενώ στη συνέχεια επεκτάθηκε για να καλύπτει τις αυξανόμενες απειλές και τις πιο προηγμένες τεχνικές επίθεσης. Σήμερα, οι Τεχνικοί ασφάλειας είναι ζωτικής σημασίας για την προστασία των πληροφοριακών συστημάτων και των δεδομένων των οργανισμών και των επιχειρήσεων.

Αξίζει να σημειωθεί ότι η πορεία και η εξέλιξη του επαγγέλματος του Τεχνικού ασφάλειας συστημάτων πληροφορικής συνεχίζεται, καθώς οι απειλές ασφάλειας εξελίσσονται διαρκώς και εμφανίζονται νέες τεχνολογίες και πρακτικές, ενώ πλέον αναπτύσσονται και επιμέρους εξειδικεύσεις στην Ασφάλεια Συστημάτων Πληροφορικής (IT Security) όπως ενδεικτικά το Network Security, το Application Security, το Cloud Security κτλ.

Οι Τεχνικοί ασφάλειας πρέπει να είναι συνεχώς ενημερωμένοι και να αναπτύσσουν τις γνώσεις και τις δεξιότητές τους, για να αντιμετωπίζουν τις απειλές και να διασφαλίζουν την ασφάλεια των πληροφοριακών συστημάτων.

Τέλος, υπάρχουν σχετικές βιβλιογραφικές και λοιπές πηγές για την ιστορική εξέλιξη του επαγγέλματος του Τεχνικού ασφάλειας συστημάτων πληροφορικής, οι οποίες ενδεικτικά περιλαμβάνουν:

- Ειδικά βιβλία για την ασφάλεια συστημάτων πληροφορικής και τον ρόλο των τεχνικών ασφάλειας, όπως:
  α] Wm. Arthur Conklin, Greg White, Chuck Cothren, Roger Davis, Dwayne Williams, (2018), Principles of Computer Security: CompTIA Security+ and Beyond, 5th Edition, Publisher, McGraw Hill
  β] William Stallings, (2019), Computer Security: Principles and Practice, Publisher Pearson
  γ] Jason Andress, (2014), The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice 2nd Edition, Publisher Syngress
- Ακαδημαϊκά άρθρα από επιστημονικά περιοδικά που ασχολούνται με την ασφάλεια συστημάτων πληροφορικής και την εξέλιξη του επαγγέλματος.
- Συνέδρια και εκδηλώσεις που ασχολούνται με την ασφάλεια συστημάτων πληροφορικής. Πολλά από αυτά τα συνέδρια παρέχουν πρακτικές πληροφορίες και αναλύσεις για τις τελευταίες εξελίξεις και τάσεις στον τομέα.
- Ιστοσελίδες και ιστότοποι ασφάλειας Πληροφορικής, που μπορούν να παρέχουν άρθρα, οδηγούς και άλλα υλικά για τον τομέα της ασφάλειας συστημάτων πληροφορικής.

## Α.5 Οικονομία και επιχειρηματικό περιβάλλον

Συγκεκριμένα στατιστικά και αριθμητικά στοιχεία αναφορικά με τον αριθμό των ατόμων που δραστηριοποιούνται στο επάγγελμα του Τεχνικού ασφάλειας συστημάτων πληροφορικής, γεωγραφική κατανομή τους κτλ. δεν υφίστανται επίσημα καταγεγραμμένα.

Περαιτέρω, ο ρόλος του Τεχνικού ασφάλειας συστημάτων πληροφορικής είναι ζωτικής σημασίας στην εποχή της ψηφιακής ανάπτυξης και της αυξημένης κυβερνοασφάλειας. Υπάρχουν ορισμένες τάσεις που επηρεάζουν το επάγγελμα του Τεχνικού ασφάλειας συστημάτων πληροφορικής στην ελληνική, ευρωπαϊκή και διεθνή αγορά. Ορισμένες από αυτές περιλαμβάνουν:

Αυξημένη ζήτηση: Οι απειλές κυβερνοασφάλειας αυξάνονται διαρκώς και ως αποτέλεσμα, υπάρχει μια αυξημένη ζήτηση για Τεχνικούς ασφάλειας συστημάτων πληροφορικής. Οι εταιρείες και οργανισμοί αναζητούν ειδικούς που θα προστατεύουν τα δίκτυά τους και τα δεδομένα τους από επιθέσεις και παραβιάσεις.

Επέκταση της νομοθεσίας και των κανονισμών: Οι νομοθετικές και κανονιστικές απαιτήσεις σχετικά με την κυβερνοασφάλεια και την προστασία δεδομένων εξελίσσονται διαρκώς, αυξάνοντας τις απαιτήσεις για συμμόρφωση των επιχειρήσεων και των οργανισμών με τα νέα νομοθετικά δεδομένα, σε εθνικό και διεθνές επίπεδο.

Τάση προς την αυτοματοποίηση και τον έλεγχο ασφάλειας: Η τεχνολογία της τεχνητής νοημοσύνης και της μηχανικής μάθησης χρησιμοποιείται για την ανίχνευση και την αντιμετώπιση απειλών ασφάλειας. Οι Τεχνικοί ασφάλειας συστημάτων πληροφορικής πρέπει να προσαρμοστούν σε αυτές τις νέες τάσεις και να αναπτύξουν δεξιότητες στη χρήση τέτοιων εργαλείων και τεχνολογιών.

Ανάγκη για εξειδίκευση: Οι επιθέσεις κυβερνοασφάλειας γίνονται όλο και πιο εξεζητημένες και σύνθετες. Αυτό δημιουργεί ανάγκη για ειδικούς που έχουν εξειδίκευση και βαθιά γνώση σε συγκεκριμένους τομείς της κυβερνοασφάλειας, όπως ο εντοπισμός ευπαθειών των πληροφοριακών συστημάτων, η ανάλυση κακόβουλου λογισμικού και η αντιμετώπιση προηγμένων απειλών.

Το επάγγελμα του Τεχνικού ασφάλειας συστημάτων πληροφορικής επηρεάζεται σημαντικά από τις τεχνολογικές αλλαγές και τις εξελίξεις στον τομέα της πληροφορικής και της κυβερνοασφάλειας. Ορισμένες από τις τεχνολογίες και τις τεχνολογικές αλλαγές που έχουν σημαντική επίδραση στο επάγγελμα έχουν ως εξής:

Εξελίξεις στον τομέα του υπολογιστικού νέφους (cloud computing): Η χρήση του υπολογιστικού νέφους (cloud computing) έχει επηρεάσει τον τρόπο λειτουργίας και διαχείρισης των πληροφοριακών συστημάτων. Οι Τεχνικοί ασφάλειας πρέπει να αντιμετωπίσουν προκλήσεις, όπως, η ασφάλεια των δεδομένων στο υπολογιστικό νέφος, η προστασία των προσβάσεων και η ασφάλεια των εφαρμογών που λειτουργούν σε αυτό.

Ανάπτυξη του Internet of Things (IoT): Οι διασυνδεδεμένες συσκευές IoT δημιουργούν νέες προκλήσεις στον τομέα της ασφάλειας. Οι Τεχνικοί ασφάλειας πρέπει να αντιμετωπίσουν τις απειλές από την εκτεταμένη συνδεσιμότητα των συσκευών IoT και να εξασφαλίσουν την ασφάλεια των δεδομένων που ανταλλάσσονται μεταξύ αυτών των συσκευών.

Ανάπτυξη της τεχνητής νοημοσύνης (AI): Η τεχνητή νοημοσύνη έχει επηρεάσει την ασφάλεια πληροφοριών, καθώς παρέχει τη δυνατότητα ανίχνευσης και αντιμετώπισης προηγμένων κυβερνοαπειλών. Οι Τεχνικοί ασφάλειας πρέπει να εκμεταλλευτούν την τεχνητή νοημοσύνη για την ανίχνευση και την αντιμετώπιση κακόβουλου λογισμικού και άλλων κυβερνοαπειλών.

Εξέλιξη της κρυπτογραφίας: Η κρυπτογραφία παίζει σημαντικό ρόλο στην ασφάλεια των πληροφοριακών συστημάτων. Οι τεχνολογικές αλλαγές στους αλγόριθμους κρυπτογράφησης και οι νέες μέθοδοι κρυπτογράφησης επηρεάζουν τον τρόπο που πρέπει να προστατεύονται και κρυπτογραφούνται τα δεδομένα και οι πληροφορίες σε έναν οργανισμό.

Αυτές οι τεχνολογικές αλλαγές απαιτούν από τους Τεχνικούς ασφάλειας συστημάτων πληροφορικής να είναι ενημερωμένοι και καταρτισμένοι σε αυτές τις νέες τεχνολογίες, ώστε να μπορούν να αντιμετωπίσουν τις απειλές και να εφαρμόσουν αποτελεσματικά μέτρα ασφάλειας.

Επισημαίνεται, περαιτέρω, ότι η κλιματική αλλαγή και η περιβαλλοντική προστασία έχουν επιδράσει στον τομέα της πληροφορικής και ασφάλειας των πληροφοριών. Ορισμένες εξελίξεις που επηρεάζουν το επάγγελμα του Τεχνικού ασφάλειας συστημάτων πληροφορικής σε σχέση με την κλιματική αλλαγή και την περιβαλλοντική προστασία περιλαμβάνουν:

Αυξημένος κίνδυνος κυβερνοαπειλών: Η κλιματική αλλαγή μπορεί να έχει αντίκτυπο στην αύξηση των κυβερνοαπειλών. Οι φυσικές καταστροφές και οι ακραίες καιρικές συνθήκες μπορούν να οδηγήσουν σε αυξημένο κίνδυνο κυβερνοεπιθέσεων. Οι Τεχνικοί ασφάλειας πρέπει να προετοιμαστούν για αυτούς τους κινδύνους και να εφαρμόζουν αποτελεσματικά μέτρα ασφάλειας για την προστασία των πληροφοριών και των συστημάτων.

Ανάγκη για περιβαλλοντικά βιώσιμες λύσεις: Οι οργανισμοί αναζητούν λύσεις που είναι περιβαλλοντικά βιώσιμες και παράλληλα ασφαλείς για τα πληροφοριακά τους συστήματα. Οι Τεχνικοί ασφάλειας πρέπει να εφαρμόζουν πρακτικές ασφάλειας που είναι συμβατές με την περιβαλλοντική προστασία, όπως η αποτελεσματική διαχείριση των αποβλήτων ηλεκτρονικών συσκευών και η προαγωγή της ανακύκλωσης.

Αποδοτικότητα ενέργειας και υπολογιστική ισχύς: Η ανάπτυξη πιο αποδοτικών συστημάτων υπολογιστών και δικτύων μπορεί να έχει θετικό αντίκτυπο στη μείωση της ενεργειακής κατανάλωσης. Οι Τεχνικοί ασφάλειας μπορούν να συμβάλουν στη μείωση της κατανάλωσης ενέργειας και τη βελτίωση της απόδοσης των πληροφοριακών συστημάτων, ενώ διατηρούν την απαραίτητη ασφάλεια.

Οι εξελίξεις αυτές απαιτούν από τους Τεχνικούς ασφάλειας συστημάτων πληροφορικής να είναι ενημερωμένοι και να προσαρμόζονται στις νέες προκλήσεις που προκύπτουν από την κλιματική αλλαγή και την περιβαλλοντική προστασία.

Τέλος, ένα βασικό πρότυπο που θα πρέπει να έχει υπόψη του ο Τεχνικός ασφάλειας συστημάτων πληροφορικής είναι το ISO 27001/2022 «Information security, cybersecurity and privacy protection – Information security management systems – Requirements»[5]. Το ISO 27001/2022 είναι ένα διεθνές πρότυπο ποιότητας για την ασφάλεια των πληροφοριών, το οποίο αναπτύχθηκε από τον Διεθνή Οργανισμό Προτύπων (ISO) και καθορίζει τις απαιτήσεις για την ίδρυση, εφαρμογή, λειτουργία, παρακολούθηση, αναθεώρηση, συντήρηση και βελτίωση ενός συστήματος διαχείρισης ασφάλειας των πληροφοριών (ISMS).

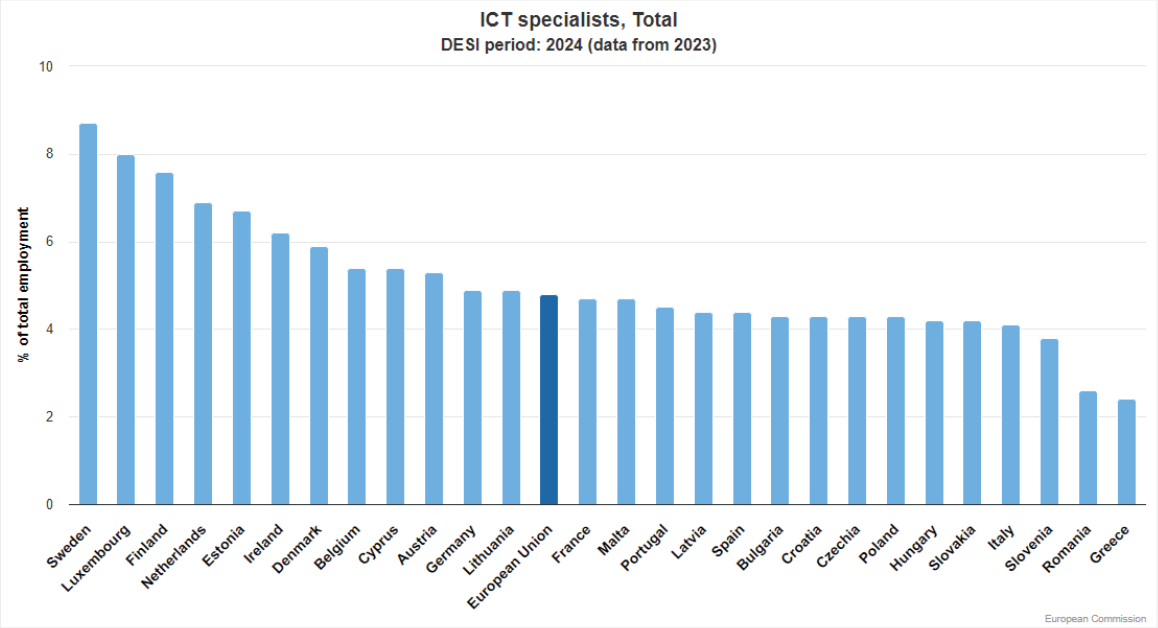
## Α.6 Εργασία, ανθρώπινο δυναμικό και συνθήκες απασχόλησης

Η ανάγκη του ψηφιακού μετασχηματισμού της χώρας μας και οι επενδύσεις των εταιρειών στην τεχνολογία έχουν οδηγήσει σε αύξηση της ζήτησης για στελέχη πληροφορικής, ωστόσο, η Ελλάδα δεν απασχολεί αρκετούς εργαζομένους στον κλάδο αυτό και καταγράφει μάλιστα αρνητική πρωτιά σε σχέση με άλλες ευρωπαϊκές χώρες.

Σύμφωνα με στοιχεία της Eurostat, το 2023, στην Ελλάδα, το ποσοστό των εργαζομένων στον κλάδο των τεχνολογιών πληροφορικής και επικοινωνίας (ΤΠΕ), ως προς το σύνολο των απασχολουμένων, αγγίζει το 2,4%,

[5] https://www.iso.org/standard/27001 (Ημερομηνία πρόσβασης: 1/7/2023)

καταγράφοντας τη χαμηλότερη επίδοση στην Ε.Ε., ενώ ειδικότερα ως προς τους εργαζομένους στην ασφάλεια συστημάτων πληροφορικής, δεν διατίθενται ακριβή και έγκυρα στοιχεία για τον αριθμό απασχολούμενων στο επάγγελμα, έκταση αυτοαπασχόλησης και γεωγραφική κατανομή των απασχολουμένων κτλ.




*Εικόνα 1: Ποσοστό ειδικών στο τομέα των Τεχνολογιών Πληροφορικής και Επικοινωνιών (Πηγή: Eurostat)*

Τη δεύτερη χαμηλότερη επίδοση έχει η Ρουμανία με 2,6%, ενώ ακολουθεί η Σλοβενία με μόλις το 3,8% των εργαζομένων στη χώρα να απασχολείται στον συγκεκριμένο κλάδο. Αντιθέτως, τα υψηλότερα ποσοστά στελεχών του κλάδου της πληροφορικής καταγράφει η Σουηδία (8,7%), το Λουξεμβούργο (8%) και η Φινλανδία (7,6%)[6].

Συνολικά, μετά και την πανδημική κρίση, οι ειδικοί της πληροφορικής έχουν αυξηθεί στην Ε.Ε. Το 2023, 9,8 εκατομμύρια άτομα απασχολούνταν στον κλάδο ΤΠΕ, αντιπροσωπεύοντας συνολικά το 4,8% του αριθμού των εργαζομένων. Τη δεκαετία 2012-2022 ο αριθμός των ειδικών στην πληροφορική αυξήθηκε κατά 57,8%, ποσοστό 6,6 φορές μεγαλύτερο σε σχέση με το ποσοστό αύξησης της απασχόλησης στην Ε.Ε. (+8,8%). Ο κλάδος της τεχνολογίας απασχολεί μόλις το 2,5% του συνόλου των εργαζομένων, ποσοστό που είναι το δεύτερο χαμηλότερο στην Ε.Ε.

Έρευνα που διεξήγαγε η Deloitte[7] για λογαριασμό του Συνδέσμου Επιχειρήσεων Πληροφορικής και Επικοινωνιών Ελλάδος (ΣΕΠΕ), δείχνει πως η ελληνική αγορά έως το 2030 θα χρειαστεί 300.000 επαγγελματίες και τεχνικούς πληροφορικής, συμπεριλαμβανομένων και Τεχνικών ασφάλειας συστημάτων πληροφορικής, που καλούνται να συμβάλλουν στον ψηφιακό μετασχηματισμό της χώρας. Έτσι, υπάρχει ανάγκη για επιπλέον 15.000-16.000 ειδικούς του κλάδου, ετησίως, μέχρι τότε, τη στιγμή που η προσφορά είναι της τάξης των 8.000-8.500. Άρα, παρουσιάζεται ένα κενό μεταξύ ζήτησης και προσφοράς, 7.000 με 7.500 άτομα. Η αδυναμία του εκπαιδευτικού συστήματος να ανταποκριθεί στις ανάγκες της οικονομίας και της αγοράς, εξηγεί, εν μέρει, τα μικρά ποσοστά απασχόλησης εργαζομένων ΤΠΕ στην Ελλάδα.

Όπως αναφέρει η ίδια έρευνα, η μη επαρκής εξειδίκευση σε συγκεκριμένα γνωστικά αντικείμενα, ο ελλιπής επαγγελματικός προσανατολισμός στη δευτεροβάθμια εκπαίδευση, οι περιορισμένες ευκαιρίες επαγγελματικής κατάρτισης σε γνωστικά αντικείμενα ΤΠΕ, καθώς και ο μικρός αριθμός εισακτέων σε συναφή τμήματα ελληνικών ΑΕΙ εξηγούν τους λόγους έλλειψης στελεχών από την ελληνική αγορά. Εδώ προστίθεται και η μετανάστευση των επιστημόνων στο εξωτερικό.

Το επίπεδο των αμοιβών για τους Τεχνικούς ασφάλειας συστημάτων πληροφορικής μπορεί να διαφέρει αισθητά, ανάλογα με διάφορους παράγοντες, όπως η χώρα/περιοχή εργασίας, το επίπεδο εμπειρίας, η εξειδίκευση και οι

[6] DESI indicators - Digital Decade DESI visualisation tool

[7] https://www2.deloitte.com/content/dam/Deloitte/gr/Documents/consulting/gr_assessment_study_on_the%20capacity_of_ict_specialists_noexp.pdf (Ημερομηνία πρόσβασης: 1/7/2023)

πιστοποιήσεις που διαθέτει κάποιος επαγγελματίας. Επιπλέον, η μεγάλη "ψαλίδα" μεταξύ προσφοράς και ζήτησης στον τομέα της κυβερνοασφάλειας μπορεί να επηρεάσει σημαντικά τα επίπεδα αμοιβών.

Σε ανεπτυγμένες χώρες ή περιοχές με υψηλή ζήτηση για ειδικούς ασφάλειας, οι αμοιβές μπορεί να είναι αρκετά ανταγωνιστικές. Εξειδικευμένοι και έμπειροι Τεχνικοί ασφάλειας μπορούν να έχουν αξιοσημείωτες αμοιβές, ιδιαίτερα αν έχουν πιστοποιήσεις και εμπειρία σε σημαντικά έργα ασφάλειας.

Επιπλέον, η άνοδος ή η πτώση της ζήτησης στον τομέα της κυβερνοασφάλειας και οι νέες τάσεις στην τεχνολογία μπορούν να επηρεάσουν τις αμοιβές. Για παράδειγμα, αν υπάρχει ένα νέο είδος κυβερνοαπειλής που απαιτεί ειδικές γνώσεις, οι ειδικοί που διαθέτουν αυτές τις δεξιότητες μπορεί να ζητούν αυξημένες αμοιβές. Περαιτέρω, αναφορικά με τα μέτρα ασφάλειας τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ - ICT) που λαμβάνουν οι επιχειρήσεις σε Ελλάδα και Ευρωπαϊκή Ένωση, η Eurostat δημοσίευσε μια ενδιαφέρουσα έρευνα[8]. Σύμφωνα με αυτήν, το 2019, το 93% των επιχειρήσεων στην ΕΕ, με 10 ή περισσότερους εργαζόμενους, χρησιμοποιούσε τουλάχιστον ένα μέτρο ασφάλειας ΤΠΕ σε επίπεδο ελέγχου ή διαδικασίας, προκειμένου να διασφαλιστεί η ακεραιότητα, η γνησιότητα, η διαθεσιμότητα και η εμπιστευτικότητα των δεδομένων και των πληροφοριακών συστημάτων της. Η Ελλάδα βρίσκεται πολύ χαμηλά στη συγκεκριμένη λίστα, με 74%, μπροστά μόνο από Ρουμανία (73%) και Μαυροβούνιο (69%).

Σύμφωνα με τα στοιχεία της Eurostat, οι μεγάλες επιχειρήσεις (με 250 εργαζόμενους και πάνω) είναι πιο πιθανό να αντιμετωπίσουν προβλήματα, λόγω συμβάντων που σχετίζονται με την ασφάλεια των ΤΠΕ, καθώς σχεδόν το ένα τέταρτο (23%) αντιμετώπισε, τουλάχιστον μία φορά προβλήματα, λόγω τέτοιου είδους περιστατικών, το 2018, σε σύγκριση με μία στις έξι μεσαίες επιχειρήσεις (17%) και μία στις δέκα μικρές (11%).

Μία στις οκτώ επιχειρήσεις (12%) αντιμετώπισε, τουλάχιστον μία φορά, προβλήματα λόγω των συμβάντων που σχετίζονται με την ασφάλεια των ΤΠΕ, το 2018. Το πιο συχνά αναφερόμενο πρόβλημα που προκλήθηκε από συμβάντα ασφάλειας ΤΠΕ είχε σχέση με τη διαθεσιμότητα υπηρεσιών, όπως π.χ. αποτυχίες υλικού ή λογισμικού, επιθέσεις άρνησης υπηρεσιών (DOS), επιθέσεις με ransomware, επηρεάζοντας το 9% των επιχειρήσεων. Ακολουθεί η καταστροφή ή φθορά δεδομένων, λόγω μόλυνσης από κακόβουλο λογισμικό, αποτυχίες λογισμικού ή υλισμικού ή μη εξουσιοδοτημένη πρόσβαση (5% των επιχειρήσεων) και λιγότερο συχνά οι επιχειρήσεις (1%) ανέφεραν την αποκάλυψη εμπιστευτικών πληροφοριών, εξαιτίας εισβολής στα συστήματα, pharming ή phishing.

Το επάγγελμα του Τεχνικού ασφάλειας συστημάτων πληροφορικής είναι ένα επάγγελμα με δυναμισμό και ανάπτυξη. Υπάρχουν διάφοροι παράγοντες που συντελούν στον δυναμισμό του, όπως:

Αυξημένη ζήτηση: Η ανάπτυξη της ψηφιακής εποχής και η αυξανόμενη εξάπλωση των πληροφοριακών συστημάτων έχουν οδηγήσει σε αυξημένη ζήτηση για Τεχνικούς ασφάλειας συστημάτων πληροφορικής. Οι οργανισμοί αναζητούν εξειδικευμένους επαγγελματίες για την προστασία των πληροφοριών τους από κυβερνοαπειλές και παραβιάσεις ασφάλειας.

Συνεχής εξέλιξη των απειλών: Οι κυβερνοαπειλές εξελίσσονται συνεχώς και γίνονται όλο και πιο εξειδικευμένες και επικίνδυνες. Αυτό δημιουργεί την ανάγκη για συνεχή εκπαίδευση και εξειδίκευση των Τεχνικών ασφάλειας συστημάτων πληροφορικής, προκειμένου να είναι σε θέση να αντιμετωπίζουν αποτελεσματικά αυτές τις απειλές.

Ανάπτυξη νέων τεχνολογιών: Η ταχεία ανάπτυξη νέων τεχνολογιών, όπως, το υπολογιστικό νέφος (cloud computing), η τεχνολογία Internet of Things (IoT) και η τεχνητή νοημοσύνη έχουν δημιουργήσει νέες προκλήσεις ασφάλειας. Οι Τεχνικοί ασφάλειας συστημάτων πληροφορικής πρέπει να είναι ενημερωμένοι και εξειδικευμένοι σε αυτές τις νέες τεχνολογίες για να προστατεύουν τα συστήματα και τις πληροφορίες από ενδεχόμενες απειλές.

Ο δυναμισμός του επαγγέλματος δημιουργεί ευκαιρίες για επαγγελματική ανάπτυξη και προοπτικές απασχόλησης για τους Τεχνικούς ασφάλειας συστημάτων πληροφορικής. Ωστόσο, είναι σημαντικό να σημειωθεί ότι οι απειλές και οι απαιτήσεις στον τομέα της ασφάλειας πληροφοριών συνεχώς εξελίσσονται και οι επαγγελματίες οφείλουν να είναι διαρκώς ενημερωμένοι και προετοιμασμένοι για να ανταποκριθούν σε αυτές τις αλλαγές.

Η επιχειρηματική προοπτική του επαγγέλματος του Τεχνικού ασφάλειας συστημάτων πληροφορικής είναι αρκετά ευνοϊκή, καθώς υπάρχει συνεχής αύξηση της ζήτησης για εξειδικευμένους επαγγελματίες στον τομέα της κυβερνοασφάλειας. Παράλληλα, οι επιθέσεις και οι απειλές στην κυβερνοασφάλεια εξελίσσονται συνεχώς,

[8] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f (Ημερομηνία πρόσβασης: 8/7/2023)

καθιστώντας το πεδίο απαιτητικό, με ανάγκες συνεχούς εκπαίδευσης και ενημέρωσης, ενώ ταυτόχρονα υπάρχει αυξημένη ζήτηση για ειδικευμένους επαγγελματίες του χώρου.

Οι συνθήκες εργασίας του Τεχνικού ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist) είναι αρκετά καλές, αρκεί να τηρούνται οι όροι ασφάλειας και οι κανονισμοί που ισχύουν για εργαζόμενους σε υπολογιστικά συστήματα. Ιδιαίτερη σημασία έχει η τήρηση των ορίων έκθεσης σε σχετικές ακτινοβολίες. Σε αρκετές περιπτώσεις, μέσα από κλαδικές συλλογικές συμβάσεις, έχει αναγνωριστεί το επίδομα ανθυγιεινής εργασίας και ειδική άδεια για όσους εργάζονται σε οθόνες υπολογιστών. Ωστόσο, αμελητέα δεν θα πρέπει να είναι η επιβάρυνση που μπορεί δεχθεί ένας Τεχνικός ασφάλειας συστημάτων πληροφορικής από την έντονη ψυχολογική πίεση που ασκείται κατά τη διάρκεια «επίθεσης» και «διαχείρισης της κρίσης», σε κάθε περιστατικό παραβίασης ασφάλειας, λαμβάνοντας υπόψη ότι ήδη έχουν αυξηθεί εκθετικά σε εύρος, σε διάρκεια και σε πολυπλοκότητα, αλλά κυρίως και σε επιπτώσεις, τα περιστατικά κυβερνοασφάλειας.

Τέλος, υπάρχουν δυνατότητες απασχόλησης στο επάγγελμα για άτομα με αναπηρία (ΑμεΑ), υπό τον όρο ότι διαθέτουν τις απαραίτητες γνώσεις και δεξιότητες που απαιτούνται για αυτό. Η αναπηρία δεν πρέπει να αποτελεί εμπόδιο για να ασκήσει κάποιος το επάγγελμα, ωστόσο επισημαίνεται ότι θα πρέπει να υπάρχουν και οι σχετικές παροχές από τον εργοδότη για άτομα με αναπηρία, οι οποίες μπορεί να ποικίλουν, ανάλογα με τον χώρο εργασίας και οι οποίες στοχεύουν να διευκολύνουν την απασχόληση των ΑμεΑ και να εξασφαλίσουν ότι διαθέτουν ισότιμες ευκαιρίες στον χώρο εργασίας. Ορισμένα παραδείγματα τέτοιων παροχών που μπορεί να παρέχονται είναι:

Προσαρμογή του χώρου εργασίας: Οι εργοδότες μπορούν να προσαρμόσουν τον χώρο εργασίας ώστε να είναι προσβάσιμος και φιλικός προς τα άτομα με αναπηρία. Αυτό μπορεί να περιλαμβάνει ράμπες, αντιολισθητικά πατώματα, προσαρμοσμένα ύψη εργασίας κ.ά.

Τεχνολογικές προσαρμογές: Παροχή τεχνολογικών εργαλείων και συσκευών που μπορούν να βοηθήσουν τα άτομα με αναπηρία στην εκτέλεση των εργασιών τους, για παράδειγμα, προσαρμοσμένα πληκτρολόγια, ποντίκια, οθόνες αφής κ.ά.

Ευέλικτο ωράριο εργασίας: Παροχή ευελιξίας στο ωράριο εργασίας, ώστε να επιτρέπεται στα άτομα με αναπηρία να προσαρμόζουν την εργασία τους στις ανάγκες τους.

Εξειδικευμένη κατάρτιση: Παροχή επιπλέον κατάρτισης ή εκπαίδευσης για την ανάπτυξη των δεξιοτήτων που απαιτούνται για την εκτέλεση των καθηκόντων της θέσης εργασίας.

## Α.7 Συνδικαλιστικές ή επιστημονικές οργανώσεις σχετικές με το επάγγελμα, έντυπα ή άλλα μέσα ή πηγές πληροφόρησης

Φορείς, ενώσεις & επιστημονικές οργανώσεις σε εθνικό επίπεδο

Τόσο οι επαγγελματίες Πληροφορικής γενικότερα, όσο και οι Τεχνικοί Ασφάλειας Συστημάτων Πληροφορικής ειδικότερα, δεν έχουν κάποια συγκεκριμένη οργάνωση ή φορέα που τους εκπροσωπεί πανελλαδικώς και αυτό ισχύει κυρίως γιατί δεν υπάρχει συγκεκριμένο πλαίσιο αδειοδότησης και άσκησης οποιασδήποτε έκφανσης του επαγγέλματος της Πληροφορικής.

Υπάρχουν τα παρακάτω συλλογικά όργανα που θα μπορούσαν, εν γένει, να εκπροσωπήσουν τους επαγγελματίες του κλάδου:

- Ελληνική Εταιρεία Επιστημόνων και Επαγγελματιών Πληροφορικής και Επικοινωνιών (ΕΠΥ - http://www.epy.gr)
- Ένωση Πληροφορικών Ελλάδος (ΕΠΕ - https://www.epe.org.gr)
- Ελληνικό Δίκτυο Επαγγελματιών Πληροφορικής (HEPIS - https://www.hepis.gr)
- Οργανισμός Ανοιχτών Τεχνολογιών (ο οποίος έχει ως κύριο στόχο να συμβάλλει στην ανοιχτότητα και ειδικότερα στην προώθηση και ανάπτυξη των Ανοιχτών Προτύπων, του Ελεύθερου Λογισμικού, του Ανοιχτού Περιεχομένου, των Ανοιχτών Δεδομένων και των Τεχνολογιών Ανοιχτής Αρχιτεκτονικής στο χώρο της εκπαίδευσης, του δημόσιου τομέα, των επιχειρήσεων και της Κοινωνικής Οικονομίας στην Ελλάδα) (ΕΕΛΛΑΚ - https://eellak.ellak.gr/)

Οι ακόλουθες ενώσεις αφορούν επαγγελματίες πληροφορικής, αλλά η εστίαση είναι σε συγκεκριμένες κατηγορίες εργαζομένων ή πτυχιούχους:

- Ένωση Μηχανικών Πληροφορικής και Επικοινωνιών Ελλάδας (ΕΜηΠΕΕ - https://www.computer-engineers.gr)
- Ελληνική Επιστημονική Ένωση Τεχνολογιών Πληροφορίας & Επικοινωνιών στην Εκπαίδευση (ΕΤΠΕ - https://www.etpe.gr)
- Πανελλήνια Ένωση Καθηγητών Πληροφορικής Δευτεροβάθμιας Εκπαίδευσης (Π.Ε.ΚΑ.Π. - http://www.pekap.gr)
- Τεχνικό Επιμελητήριο Ελλάδας (ΤΕΕ - https://web.tee.gr), τμήμα Ηλεκτρολόγων/Ηλεκτρονικών Μηχανικών και Πληροφορικής.

Σε κλαδικό επίπεδο, ο Σύνδεσμος Επιχειρήσεων Πληροφορικής & Επικοινωνιών Ελλάδας (ΣΕΠΕ - http://www.sepe.gr) και ο Σύνδεσμος Επιχειρήσεων Πληροφορικής Βορείου Ελλάδος (ΣΕΠΒΕ - http://www.sepve.org) έχουν ως μέλη επιχειρήσεις του κλάδου Ψηφιακής Τεχνολογίας και ως βασικό σκοπό την έρευνα για την ανάπτυξη σε όλους τους τομείς των Τεχνολογιών Πληροφορικής και Επικοινωνιών και την υποστήριξη και λειτουργία των επιχειρήσεων του κλάδου.

Υπάρχουν επίσης ορισμένοι οργανισμοί (π.χ. Κέντρα Δια Βίου Μάθησης, Κολλέγια, ΙΕΚ)[9] που εποπτεύονται από τον Εθνικό Οργανισμό Πιστοποίησης Προσόντων & Επαγγελματικού Προσανατολισμού (Ε.Ο.Π.Π.Ε.Π. - https://www.eoppep.gr/) και προσφέρουν εκπαίδευση και πιστοποίηση προσόντων.

Από την παράθεση των παραπάνω οργανισμών είναι σαφές ότι κάθε ένωση εκπροσωπεί συγκεκριμένες κατηγορίες του κλάδου, με την ΕΠΥ, την ΕΠΕ και την HEPIS να αποτελούν τους πιο γενικούς φορείς. Η ΕΠΥ και η ΕΠΕ απαιτούν την κατοχή τριτοβάθμιου τίτλου πληροφορικής για την εγγραφή νέου μέλους. Και οι τρείς έχουν κατά βάση τη μορφή σωματείου με παρόμοιους σκοπούς και δράσεις.

Φορείς/οργανώσεις σε ευρωπαϊκό επίπεδο

Οι κυριότερες οργανώσεις σε ευρωπαϊκό επίπεδο που αφορούν σε επαγγελματίες πληροφορικής ή σε ψηφιακές δεξιότητες είναι:

- Council of European Professional Informatics Societies (CEPIS – http://www.cepis.org)
- European e-Skills Association (EeSA - http://eskillsassociation.eu)
- UNI Europa - European services workers union (http://www.uni-europa.org)
- Computer & Communications Industry Association (CCIA - https://www.ccianet.org)

Ο φορέας HEPIS (www.hepis.gr), που αναφέραμε πιο πάνω, είναι το τοπικό παρακλάδι του φορέα CEPIS.

Υπάρχουν και άλλες Ενώσεις Πληροφορικής σε ευρωπαϊκό επίπεδο, αλλά έχουν κυρίως ερευνητικό προσανατολισμό και δεν αφορούν σε επαγγελματικές πτυχές του κλάδου.

## Α.8 Θεσμικό πλαίσιο λειτουργίας του επαγγέλματος

Αρχικά πρέπει να αναφερθεί ότι δεν υπάρχει μέχρι σήμερα κάποια θεσμοθετημένη επαγγελματική άδεια ή προαπαιτούμενο για την άσκηση επαγγελμάτων Πληροφορικής, εν γένει, και του Τεχνικού ασφάλειας συστημάτων πληροφορικής συμπεριλαμβανομένου, δηλαδή δεν απαιτείται η εγγραφή σε κάποιο μητρώο ή κάποια ειδική αδειοδότηση για την άσκηση του επαγγέλματος.

Αναφορικά με τον τρόπο άσκησης του επαγγέλματος και ειδικότερα θέματα που αφορούν στο αντικείμενο εργασίας του επαγγελματία της ειδικότητας, ενδέχεται στην περίπτωση εξαρτημένης εργασίας, να καθορισθούν από τον εργοδότη στη σύμβαση εξαρτημένης εργασίας.

Στο σημείο αυτό πρέπει να επισημανθεί ότι στην Ευρώπη δεν υπάρχουν συγκεκριμένοι κανονισμοί και προϋποθέσεις για την άσκηση του επαγγέλματος, δηλαδή δεν υπάρχει θεσμική απαίτηση για συγκεκριμένη αδειοδότηση.

[9] Ιδιωτικοί φορείς εκπαίδευσης και κατάρτισης, https://bit.ly/32mMOiE (Ημερομηνία πρόσβασης: 10/7/2023)

Όπως σε ευρωπαϊκό επίπεδο υπάρχουν σχετικές Οδηγίες και Κανονισμοί για το αντικείμενο της Πληροφορικής, έτσι και στην Ελλάδα (όπου οι σχετικές Οδηγίες και Κανονισμοί έχουν ενσωματωθεί), ο επαγγελματίας της ειδικότητας θα πρέπει γνωρίζει αντικείμενα που επηρεάζουν άμεσα το επάγγελμα του και αυτά είναι θέματα που σχετίζονται:

- με τα προσωπικά δεδομένα (GDPR), τα τεχνικά - οργανωτικά μέτρα ασφάλειας πληροφοριών/δεδομένων, την ύπαρξη πολιτικής και σχεδίου ασφάλειας και τον ρόλο του υπευθύνου προστασίας δεδομένων (DPO) σε μια επιχείρηση/οργανισμό (Νόμος 4624/2019 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων»).

- με τον Κανονισμό (ΕΕ) 2023/2854 (Data Act) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2023, για εναρμονισμένους κανόνες σχετικά με τη δίκαιη πρόσβαση σε δεδομένα και τη δίκαιη χρήση τους και για την τροποποίηση του κανονισμού (ΕΕ) 2017/2394 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για τα δεδομένα **(**https://eur-lex.europa.eu/eli/reg/2023/2854**).**

- με τον Κανονισμό (ΕΕ) του 2019/881 (Cybersecurity Act) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ) **(**https://eur-lex.europa.eu/eli/reg/2019/881/oj?locale=el**)**

- με τον Κανονισμό (ΕΕ) 910/2014 (eIDAS) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014 , σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ **(**https://eur-lex.europa.eu/eli/reg/2014/910/oj**)**

- με την Οδηγία (ΕΕ) 2016/1148 που εκδόθηκε τον Ιούλιο 2016 στο πλαίσιο της ευρωπαϊκής στρατηγικής για την ασφάλεια στον κυβερνοχώρο, με στόχο την επίτευξη υψηλού κοινού επιπέδου ασφάλειας για τις κρίσιμες υποδομές σε ολόκληρη την ΕΕ. Η Οδηγία, ευρέως γνωστή ως NIS (από τα αρχικά «Network and Information Systems»), θεσπίζει μέτρα ασφάλειας και συνέχειας για τα συστήματα δικτύου και πληροφοριών που υποστηρίζουν την παροχή υπηρεσιών με σοβαρό αντίκτυπο στην ομαλή και εύρυθμη λειτουργία της αγοράς, όπως είναι η προμήθεια ενέργειας σε άτομα και επιχειρήσεις εντός της Ένωσης. Η Ευρωπαϊκή Οδηγία ενσωματώθηκε στην ελληνική νομοθεσία το Δεκέμβριο 2018, με το νόμο 4577/2018. Θέματα εφαρμογής του εθνικού νόμου εξειδικεύτηκαν περαιτέρω με την Υπουργική Απόφαση 1027/2019.
- με την πνευματική ιδιοκτησία (copyright) και τις άδειες Creative Commons (Νόμος 2121/1993 «Πνευματική Ιδιοκτησία, Συγγενικά Δικαιώματα και Πολιτιστικά Θέματα»).
- με την ηλεκτρονική/ψηφιακή διακυβέρνηση [Νόμος 4727/2020 - Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις).
- με ρυθμίσεις σχετικά με την Τεχνητή Νοημοσύνη, την Κυβερνοασφάλεια, το Διαδίκτυο των πράγματων (Internet Of Things/IoT), την τεχνολογία blockchain και το 3D printing (Νόμος 4961/2022 «Αναδυόμενες

τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις»).

**Νομοθεσία και θεσμικά κείμενα σχετικά με την Πληροφορική και την Ασφάλεια Συστημάτων Πληροφορικής**

- Νόμος 5086/2024 (Α' 23) - Εθνική Αρχή Κυβερνοασφάλειας και λοιπές διατάξεις.
- Νόμος 4624/2019 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων».
- Νόμος 4577/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις».
- Νόμος 4727/2020 - Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.
- Νόμος 4961/2022 «Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις».
- Νόμος 5002/2022 «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών».
- Νόμος 2121/1993 «Πνευματική Ιδιοκτησία, Συγγενικά Δικαιώματα και Πολιτιστικά Θέματα» (άδειες Creative Commons).
- Βίβλος Ψηφιακού Μετασχηματισμού 2020-2025 (https://digitalstrategy.gov.gr/ ).
- Εθνική Στρατηγική Κυβερνοασφάλειας (https://mindigital.gr/wp-content/uploads/2020/12/Εθνική-Στρατηγική-Κυβερνοασφάλειας.pdf).
- Οδηγός Αυτοαξιολόγησης της Κυβερνοασφάλειας Οργανισμών (Cybersecurity Self Assessment Tool) της Εθνικής Αρχής Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης (https://mindigital.gr/wp-content/uploads/2022/11/Cybersecurity-Self-Assessment-Tool-Greek-version.zip )
- Εγχειρίδιο Κυβερνοασφάλειας (Cybersecurity Handbook), της Εθνικής Αρχής Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης https://mindigital.gr/wp-content/uploads/2022/09/Εγχειρίδιο-Κυβερνοασφάλειας-Ελληνική-έκδοση.pdf)

## Α.9 Τεχνολογίες/τεχνολογικές αλλαγές που επηρεάζουν το επάγγελμα.

Το επάγγελμα του Τεχνικού ασφάλειας συστημάτων πληροφορικής επηρεάζεται σημαντικά από τις τεχνολογικές αλλαγές και τις εξελίξεις στον τομέα της πληροφορικής και της κυβερνοασφάλειας. Οι παρακάτω τεχνολογίες έχουν έναν μεγάλο και σημαντικό αντίκτυπο στον τρόπο λειτουργίας και τις απαιτήσεις των επαγγελματιών ασφάλειας συστημάτων πληροφορικής:

Τεχνολογίες υπολογιστικού νέφους (cloud computing): Οι υπηρεσίες και τεχνολογίες υπολογιστικού νέφους (cloud computing) επηρεάζουν το επάγγελμα του Τεχνικού ασφάλειας συστημάτων πληροφορικής, προκαλώντας νέες προκλήσεις ασφάλειας, αλλά παράλληλα παρέχοντας ευκαιρίες για την εξέλιξη και την εφαρμογή νέων πρακτικών ασφάλειας. Οι επαγγελματίες αυτού του τομέα πρέπει να είναι ενημερωμένοι και να αναπτύσσουν τις γνώσεις και τις δεξιότητές τους για να αντιμετωπίσουν τις νέες προκλήσεις και να διασφαλίσουν την ασφάλεια των πληροφοριακών συστημάτων στο περιβάλλον του υπολογιστικού νέφους.

Internet of Things (IoT) (ή άλλως η διαδικτύωση των πάντων): Η ανάπτυξη των συνδεδεμένων συσκευών και των έξυπνων αντικειμένων έχει δημιουργήσει νέες προκλήσεις ασφάλειας. Οι Τεχνικοί ασφάλειας πρέπει να αντιμετωπίζουν τις απειλές για την ασφάλεια των συνδεδεμένων συσκευών και να εξασφαλίζουν την προστασία των δεδομένων που συλλέγονται.

Τεχνητή Νοημοσύνη (artificial intelligence) και Μηχανική Μάθηση: Οι αλγόριθμοι Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης χρησιμοποιούνται για την ανίχνευση και αντιμετώπιση απειλών. Οι Τεχνικοί ασφάλειας πρέπει να είναι εξοικειωμένοι με αυτές τις τεχνολογίες και να τις εφαρμόζουν για να αντιμετωπίζουν τις απειλές ασφάλειας πιο αποτελεσματικά.

Κινητές Εφαρμογές και Bring Your Own Device (BYOD): Η χρήση κινητών συσκευών και η εφαρμογή του μοντέλου BYOD έχουν αυξήσει την πολυπλοκότητα της ασφάλειας. Οι Τεχνικοί ασφάλειας πρέπει να αναπτύξουν πολιτικές και μέτρα ασφάλειας για τη διαχείριση των κινητών συσκευών και των εφαρμογών τους.

Τεχνολογίες Κατανεμημένου Καθολικού (Distributed Ledger Technology - DLT) - (Blockchain) Οι τεχνολογίες κατανεμημένου καθολικού (Blockchain) παρέχουν ασφάλεια και εμπιστοσύνη στις διαδικτυακές συναλλαγές. Οι Τεχνικοί ασφάλειας πρέπει να εξετάσουν τον τρόπο ασφαλούς υλοποίησης και τη χρήση της τεχνολογίας Blockchain στις εφαρμογές και τα συστήματα που διαχειρίζονται.

Νέες δυνατότητες δικτύωσης των δικτύων 5ης γενιάς: Η νέα τεχνολογία δικτύων 5ης γενιάς, γνωστή και ως 5G, έχει έναν σημαντικό αντίκτυπο στο επάγγελμα του Τεχνικού ασφάλειας συστημάτων πληροφορικής καθότι προσφέρουν πολλά πλεονεκτήματα, αλλά, παράλληλα, δημιουργούν νέες προκλήσεις ασφάλειας και ιδιωτικότητας. Οι επαγγελματίες αυτού του τομέα πρέπει να είναι ενημερωμένοι για τις απειλές και τις βέλτιστες πρακτικές ασφάλειας που αφορούν τα δίκτυα 5ης γενιάς και να διαθέτουν τις απαραίτητες δεξιότητες για να αντιμετωπίσουν τις προκλήσεις αυτές και να εξασφαλίσουν την ασφάλεια των δικτύων και των συνδεδεμένων συσκευών.

Απομακρυσμένη εργασία: Η απομακρυσμένη εργασία, η οποία αναφέρεται, επίσης, ως τηλεργασία ή εργασία από απόσταση, προσφέρει ευελιξία, ευκολία και πλεονεκτήματα, αλλά απαιτεί ταυτόχρονα τη λήψη πρόσθετων μέτρων ασφάλειας για την ασφάλεια και προστασία των δεδομένων των χρηστών και των συστημάτων. Οι επαγγελματίες αυτού του τομέα πρέπει να είναι ενημερωμένοι για τις πρακτικές ασφάλειας που σχετίζονται με την απομακρυσμένη εργασία και να εφαρμόζουν κατάλληλες τεχνικές και πολιτικές για να διασφαλίσουν την ασφάλεια των δικτύων και των δεδομένων.

Τεχνολογίες δεδομένων μεγάλης κλίμακας (Big data) και εξόρυξη δεδομένων (Data Mining):

Πρόληψη και ανίχνευση απειλών: Τα δεδομένα μεγάλης κλίμακας (Big data) αποτελούνται από τεράστιες ποσότητες δεδομένων που μπορούν να βοηθήσουν στην πρόληψη και ανίχνευση κυβερνοαπειλών. Οι Τεχνικοί ασφάλειας συστημάτων πληροφορικής μπορούν να χρησιμοποιήσουν τέτοια δεδομένα από διάφορες πηγές για να εντοπίσουν πρότυπα και ενδείκτες που υποδηλώνουν επιθέσεις και κακόβουλες ενέργειες στον κυβερνοχώρο.

Ανάλυση απειλών: Η εξόρυξη δεδομένων (Data mining) επιτρέπει την ανάλυση μεγάλων συνόλων δεδομένων για τον εντοπισμό τάσεων και κακόβουλων συμπεριφορών των επιτιθέμενων. Οι Τεχνικοί ασφάλειας συστημάτων πληροφορικής μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να αναπτύξουν καλύτερες αμυντικές στρατηγικές. Επίσης, μπορούν να χρησιμοποιήσουν την εξόρυξη δεδομένων για να εντοπίσουν ασυνήθιστες συμπεριφορές χρηστών που πιθανόν να υποδεικνύουν παραβίαση της ασφάλειας.

Οι τεχνολογίες δεδομένων μεγάλης κλίμακας (Big data) και εξόρυξης δεδομένων (Data Mining) παρέχουν στους Τεχνικούς ασφάλειας περισσότερα εργαλεία και πόρους για την προστασία των πληροφοριακών συστημάτων. Ωστόσο, είναι απαραίτητο να έχουν επαρκείς γνώσεις και εμπειρία στη χρήση αυτών των τεχνολογιών για να αξιοποιήσουν στο έπακρο τα πλεονεκτήματά τους και να προστατεύσουν αποτελεσματικά τα συστήματα πληροφορικής των οργανισμών.

Αρχιτεκτονική Μηδενικής Εμπιστοσύνης (Zero Trust Architecture - ZTA)

Το μοντέλο ασφάλειας Αρχιτεκτονική Μηδενικής Εμπιστοσύνης (ZTA) και ασφάλεια χωρίς περίμετρο) περιγράφει μια προσέγγιση για τη στρατηγική, το σχεδιασμό και την υλοποίηση των συστημάτων ΤΠ. Η βασική ιδέα πίσω από το μοντέλο αρχιτεκτονικής μηδενικής εμπιστοσύνης είναι «ποτέ μην εμπιστεύεσαι, πάντα να επαληθεύεις», πράγμα που σημαίνει ότι οι χρήστες και οι συσκευές δεν πρέπει να είναι εξ ορισμού αξιόπιστοι, ακόμη και αν είναι

συνδεδεμένοι σε ένα δίκτυο με άδεια, όπως ένα εταιρικό τοπικό δίκτυο, και ακόμη και αν έχουν προηγουμένως επαληθευτεί.

Τεχνολογία Ψηφιακών Διδύμων (Digital Twins - DT)

Η τεχνολογία Ψηφιακών Διδύμων (Digital Twins) ενισχύει την ασφάλεια στον κυβερνοχώρο, επιτρέποντας την προληπτική ανάλυση, την παρακολούθηση σε πραγματικό χρόνο, τον ασφαλή χειρισμό δεδομένων και τα αποτελεσματικά μέτρα αντιμετώπισης.

Όλες οι τεχνολογίες που προαναφέρθηκαν επηρεάζουν το επάγγελμα του Τεχνικού ασφάλειας συστημάτων πληροφορικής. Είναι σημαντικό για τους επαγγελματίες αυτού του τομέα να είναι ενημερωμένοι για τις τεχνολογικές εξελίξεις και να προσαρμόζουν συνεχώς τις γνώσεις και τις δεξιότητές τους για να αντιμετωπίσουν αποτελεσματικά τις αναδυόμενες απειλές και να εξασφαλίσουν την ασφάλεια των πληροφοριακών συστημάτων και δικτύων των οργανισμών, όπου εργάζονται.

## Α.10 Εξελίξεις αναφορικά με την κλιματική αλλαγή και την περιβαλλοντική προστασία που επηρεάζουν το επάγγελμα.

Η ηλεκτρονική διακυβέρνηση, ο εν εξελίξει ψηφιακός μετασχηματισμός σε όλους τους κλάδους της ανθρώπινης δραστηριότητας και της εν γένει υποστήριξης πάσης φύσεως εργασιών, με τη χρήση υπολογιστικών και ψηφιακών συστημάτων και τις αυξημένες δυνατότητες τηλεργασίας, συμβάλλει στην προστασία του περιβάλλοντος, μέσω της καλύτερης και αποδοτικότερης αξιοποίησης των πόρων (π.χ. ελαχιστοποίηση της χρήσης χαρτιού και αναλώσιμων, περιορισμός των μετακινήσεων κλπ.).

Περαιτέρω, σε ένα διαρκώς μεταβαλλόμενο κλίμα, οι Τεχνικοί Ασφάλειας Συστημάτων Πληροφορικής πρέπει να βρίσκουν πιο αποτελεσματικούς τρόπους για να σχεδιάσουν, να εφαρμόσουν και να διατηρήσουν το επίπεδο ασφάλειας των συστημάτων που υποστηρίζουν.

Τέλος, με την απόκτηση μεγαλύτερης περιβαλλοντικής συνείδησης από φορείς, εταιρίες, οργανισμούς, την ανάπτυξη της πράσινης ενέργειας, τις έξυπνες πόλεις, την ευφυή γεωργία, τις έξυπνες μεταφορές, έχουμε ως αποτέλεσμα την αναμενόμενη αύξηση στις αντίστοιχες θέσεις εργασίας.

ΕΝΟΤΗΤΑ Β

# ΑΝΑΛΥΣΗ ΕΠΑΓΓΕΛΜΑΤΟΣ/ΕΙΔΙΚΟΤΗΤΑΣ - ΠΡΟΔΙΑΓΡΑΦΕΣ

ΕΝΟΤΗΤΑ Γ

# ΑΠΑΡΑΙΤΗΤΕΣ ΓΝΩΣΕΙΣ, ΔΕΞΙΟΤΗΤΕΣ ΚΑΙ ΙΚΑΝΟΤΗΤΕΣ

ΕΝΟΤΗΤΑ Β: «Ανάλυση του επαγγέλματος ή/και ειδικότητας – Προδιαγραφές»
ΕΝΟΤΗΤΑ Γ: «Απαραίτητες γνώσεις, δεξιότητες και ικανότητες»

| ΚΕΛ 1 | ΣΧΕΔΙΑΖΕΙ, ΕΦΑΡΜΟΖΕΙ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΕΙ ΤΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ, ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ |
|---|---|
| ΕΕΛ 1.1 | ΣΧΕΔΙΑΖΕΙ ΤΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ, ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ |
| | ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΕΡΓΑΣΙΕΣ<br>**1.1.1.** Καταγράφει και απογράφει τα πληροφοριακά συστήματα και τον υπολογιστικό & δικτυακό εξοπλισμό του Οργανισμού<br>**1.1.2.**Εντοπίζει και αναγνωρίζει κίνδυνους, απειλές και ενέργειες/γεγονότα που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων και προβαίνει στην αξιολόγησή τους<br>**1.1.3.** Σχεδιάζει και προτείνει τη λήψη μέτρων προστασίας και ασφάλειας πληροφοριακών συστημάτων<br>**1.1.4.** Μελετά και προσδιορίζει τις ελάχιστες προδιαγραφές ασφάλειας των υπολογιστικών συστημάτων του Οργανισμού<br>**1.1.5.** Συμμετέχει στο σχεδιασμό, την εκπόνηση και την επικαιροποίηση της Πολιτικής Ασφάλειας. Πληροφοριακών. Συστημάτων και Προστασίας Δεδομένων του Οργανισμού.<br>**1.1.6.**Καταρτίζει και τεκμηριώνει ειδικότερες πολιτικές, διαδικασίες, τεχνικές και εγχειρίδια ασφάλειας πληροφοριακών συστημάτων του Οργανισμού.<br>**1.1.7.**Αναπτύσσει, σχεδιάζει και επικαιροποιεί σε περιοδική βάση πλάνο αντιμετώπισης και διαχείρισης τυχόν περιστατικών ασφάλειας, καθώς και ανάκτησης δεδομένων και επιχειρησιακής συνέχειας. |

ΚΡΙΤΗΡΙΑ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ

- Καταγράφει και απογράφει τα πληροφοριακά συστήματα και τον υπολογιστικό & δικτυακό εξοπλισμό του Οργανισμού που πρέπει να προστατευτούν, τόσο σε επίπεδο υλικού (hardware) και λογισμικού (software) όσο και δικτύων (networks), τηρώντας σχετικό επικαιροποιημένο κατάλογο-μητρώο (inventory).
- Εντοπίζει και αναγνωρίζει κινδύνους (ευπάθειες), απειλές και ενέργειες/γεγονότα που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων και προβαίνει στην αξιολόγησή τους, ανάλογα εάν μπορούν να επηρεάσουν/πλήξουν την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και την διαθεσιμότητα (availability) των πληροφοριών και δεδομένων του Οργανισμού, εφαρμόζοντας εργαλεία και μεθοδολογίες. ανάλυσης & διαχείρισης της επικινδυνότητας πληροφοριακών συστημάτων.
- Σχεδιάζει και προτείνει τη λήψη των ενδεδειγμένων μέτρων προστασίας και ασφάλειας, με βάση την αξιολόγηση των κινδύνων (risk assessment) που σχετίζονται με τη λειτουργία και χρήση πληροφοριακών συστημάτων και τα διεθνή πρότυπα ασφάλειας πληροφοριών (όπως ISO/IEC 27001, 27002, ISO/IEC 29151, Control Objectives for Information Technology (CobIT), Common Criteria, NIST/SP 800-53, ENISA).
- Μελετά προσεκτικά και προσδιορίζει τις ελάχιστες προδιαγραφές ασφάλειας των υπολογιστικών και πληροφοριακών συστημάτων του Οργανισμού, με βάση τα εγχειρίδια και τις οδηγίες χρήσης του κατασκευαστή, καθώς τις οδηγίες της διοίκησης του Οργανισμού ή του Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών, αν υφίσταται.
- Συμμετέχει, ενεργά, στο σχεδιασμό, την εκπόνηση και την επικαιροποίηση της Πολιτικής Ασφάλειας. Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων του Οργανισμού, προτείνοντας τη λήψη ενδεδειγμένων μέτρων ασφάλειας, σύμφωνα με τις ανάγκες του Οργανισμού, συνεργαζόμενος προς τούτο με τις οργανικές μονάδες ασφάλειας πληροφοριακών συστημάτων και πληροφορικής του Οργανισμού.
- Καταρτίζει και τεκμηριώνει εγγράφως, ακολουθώντας τα διεθνή πρότυπα ασφάλειας πληροφοριών, ειδικότερες πολιτικές, διαδικασίες, τεχνικές και εγχειρίδια ασφάλειας πληροφοριακών συστημάτων, σύμφωνα με τις ανάγκες του Οργανισμού, προκειμένου να προστατευθούν τα στοιχεία του πληροφοριακού συστήματος, αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή.
- Αναπτύσσει, σχεδιάζει και επικαιροποιεί, σε περιοδική βάση, λεπτομερές πλάνο αντιμετώπισης και διαχείρισης τυχόν περιστατικών ασφάλειας, καθώς και ανάκτησης δεδομένων και επιχειρησιακής συνέχειας που δύναται να επηρεάσουν τη διαθεσιμότητα, εμπιστευτικότητα ή/και ακεραιότητα των φυσικών ή ηλεκτρονικών πληροφοριακών στοιχείων του Οργανισμού, καταγράφοντας ενέργειες αναγνώρισης, ανίχνευσης και ανάλυσης περιστατικών, περιορισμού και εξάλειψης επιπτώσεων στον Οργανισμό και ανάκτησης δεδομένων.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

*Περιβάλλον και συνθήκες εργασίας:*
Επιχειρήσεις, Οργανισμοί, Υπηρεσίες κλπ. όπου υπάρχουν και χρησιμοποιούνται υπολογιστικά και πληροφοριακά συστήματα, καθώς και δικτυακός εξοπλισμός, Επιχειρήσεις και Οργανισμοί, που κατασκευάζουν, προωθούν - πωλούν και υποστηρίζουν προϊόντα ή υπηρεσίες πληροφορικής, Εμπορικές αντιπροσωπείες προϊόντων υπολογιστικών συστημάτων, επιχειρήσεις που παρέχουν υπηρεσίες υποστήριξης προς τρίτους ή/και παροχή συμβουλευτικών υπηρεσιών, σε θέματα IT Security, Cyber security και Security as a service κτλ.

Δύναται να διαθέτει ανεξάρτητο χώρο-γραφείο μέσα στον Οργανισμό με τον απαραίτητο και αναγκαίο εξοπλισμό πληροφορικής για την εκτέλεση των καθηκόντων του.

*Μέσα/εργαλεία/υλικά:*
- Πρότυπα καταλόγων-μητρώων καταγραφής και διαχείρισης των πληροφοριακών συστημάτων, του υπολογιστικού & δικτυακού εξοπλισμού του Οργανισμού (Digital Asset Inventories Templates)
- Λειτουργικά Συστήματα (Windows, Linux, Android κ.ά.) και πακέτα εφαρμογών/σουίτες γραφείου και βοηθητικά λογισμικά (Office, Libre Office, OpenOffice - Word, Excel, Internet, PowerPoint κλπ., Readers, Players, εργαλεία συμπίεσης - αποσυμπίεσης κλπ.)
- Συνήθης εξοπλισμός γραφείου (Διαδίκτυο, Η/Υ, τηλεφωνική συσκευή και προσωπική διεύθυνση ηλεκτρονικής αλληλογραφίας για επικοινωνία και υποστήριξη (e-mail))
- Ψηφιακά μέσα αποθήκευσης (USB, CD ή DVD)

*Παραγόμενη υπηρεσία:*
Σχεδιασμός μέτρων ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού.

*Μέθοδοι εφαρμογής και διαδικασίες:*
- Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων
- Μεθοδολογίες, εργαλεία και πρότυπα αξιολόγησης, ανάλυσης και διαχείρισης κινδύνων πληροφοριακών συστημάτων (Risk Assessment tools & toolkits)
- Διεθνή πρότυπα ασφάλειας πληροφοριών (όπως ISO/IEC 27001, 27002, ISO/IEC 29151, Control Objectives for Information Technology (CobIT), Common Criteria, NIST/SP 800-53, ENISA)
- Τεχνικά εγχειρίδια Κυβερνοασφάλειας (Cybersecurity-Handbooks) με βέλτιστες πρακτικές για την ασφάλεια, προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων
- Θεσμικό και κανονιστικό πλαίσιο (Νόμος 4624/2019 [Εφαρμογή GDPR], Νόμος 4577/2018 [Εφαρμογή Οδηγίας NIS]) για τα περιστατικά ασφάλειας και διαρροής δεδομένων και υποχρεώσεις - απαιτήσεις που απορρέουν από αυτό
- Οδηγίες του υπευθύνου ανάπτυξης
- Πλάνο εργασίας επιχείρησης
- Μητρώο/αρχείο καταγραφής στοιχείων λογισμικών ασφάλειας πληροφοριών και λειτουργιών διαχείρισης.

ΓΕΝΙΚΕΣ ΓΝΩΣΕΙΣ

Ως ελάχιστες προαπαιτούμενες Γνώσεις, Δεξιότητες και Ικανότητες για την περαιτέρω επαγγελματική εκπαίδευση, κατάρτιση ή επαγγελματική δραστηριότητα είναι αυτές που αντιστοιχούν:

- στο επίπεδο 2 του Εθνικού και Ευρωπαϊκού Πλαισίου Προσόντων (ΕΠΠ) «Αποκτά βασικές γενικές γνώσεις, που σχετίζονται με ένα πεδίο εργασίας ή σπουδής, που του επιτρέπουν να αντιλαμβάνεται τις διαδικασίες εφαρμογής βασικών καθηκόντων και οδηγιών» για τις περιπτώσεις αποφοίτων ΕΠΑΣ, Γενικού Λυκείου και ΕΠΑΛ και
- στο επίπεδο 4 του Εθνικού και Ευρωπαϊκού Πλαισίου Προσόντων (ΕΠΠ) «Αποκτά ευρύ φάσμα θεωρητικών γνώσεων και ανάλυσης πληροφοριών που του επιτρέπουν να κατανοεί το πεδίο εργασίας ή σπουδής και να εφαρμόζει στοιχεία και διαδικασίες σε ένα γενικό πλαίσιο» για τις περιπτώσεις αποφοίτων ΙΕΚ και Μεταλυκειακού Έτους- Τάξης Μαθητείας.

| ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΓΝΩΣΕΙΣ | |
|---|---|
| • Ασφάλεια πληροφοριακών συστημάτων, δικτύων και πληροφοριών<br>• Γνώσεις διασύνδεσης, συνδεσμολογίας και αρχιτεκτονικής δικτύων και υπολογιστικών συστημάτων<br>• Γνώσεις εντοπισμού και εφαρμογής ενημερώσεων και ελάχιστων προδιαγραφών ασφάλειας υπολογιστικών συστημάτων, λογισμικών και εφαρμογών | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5:<br>«Διαθέτει ευρείες, εξειδικευμένες, αντικειμενικές και θεωρητικές γνώσεις σε ένα πεδίο εργασίας ή σπουδής και έχει επίγνωση των ορίων των γνώσεων αυτών.» |

| | |
|---|---|
| • Πρότυπα ασφάλειας πληροφοριών (όπως ISO/IEC 27001, 27002, ISO/IEC 29151, Control Objectives for Information Technology (CobIT), Common Criteria, NIST/SP 800-53, ENISA)<br>• Τεχνική ορολογία (ελληνική και αγγλική). | |
| ΕΙΔΙΚΕΣ ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΓΝΩΣΕΙΣ:<br><br>Δεν υπάρχουν | |
| ΔΕΞΙΟΤΗΤΕΣ<br>• Χρήση προγραμμάτων, λογισμικών και λειτουργικών συστημάτων (προγράμματα εφαρμογών γραφείου, προγράμματα επεξεργασίας φωτογραφίας και εικόνων, προγράμματα διαχείρισης προσωπικών πληροφοριών, προγράμματα συμπίεσης/αποσυμπίεσης αρχείων, λογισμικά εφαρμογών, λογισμικά συστήματος, λειτουργικά συστήματα ανοικτού και κλειστού κώδικα κτλ.)<br>• Χρήση εργαλείων/μεθοδολογιών για διαχείριση, ανάλυση και αξιολόγηση κινδύνων (risk assessment), που σχετίζονται με τη λειτουργία και χρήση πληροφοριακών συστημάτων<br>• Συγγραφή και ανάπτυξη πολιτικών, διαδικασιών, τεχνικών και εγχειριδίων ασφάλειας πληροφοριακών συστημάτων<br>• Κατάρτιση και συντήρηση καταλόγου-μητρώου (inventory) πληροφοριακών, επικοινωνιακών και δικτυακών υποδομών και συστημάτων<br>• Τήρηση και εφαρμογή προτύπων/τεχνικών/μεθοδολογιών ασφάλειας πληροφοριών και προστασίας των δεδομένων<br>• Εφαρμογή και χρήση προτύπων, κανόνων και εργαλείων σύγχρονης και ασύγχρονης επικοινωνίας. | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5:<br><br>«Διαθέτει ευρείες, εξειδικευμένες, αντικειμενικές και θεωρητικές γνώσεις σε ένα πεδίο εργασίας ή σπουδής και έχει επίγνωση των ορίων των γνώσεων αυτών.» |

| ΨΗΦΙΑΚΕΣ ΔΕΞΙΟΤΗΤΕΣ | Επίπεδο χρήστη | Κατηγορίες Ψηφιακών Δεξιοτήτων | | | | |
|---|---|---|---|---|---|---|
| | | Επεξεργασία Δεδομένων | Δημιουργία Περιεχομένου | Επικοινωνία | Επίλυση Προβλημάτων | Ασφάλεια |
| | Βασικός | - | - | - | - | - |
| | Ανεξάρτητος | - | ✓ | - | - | - |
| | Έμπειρος | ✓ | - | ✓ | ✓ | ✓ |

| | |
|---|---|
| ΙΚΑΝΟΤΗΤΕΣ<br><br>Βασικές Ικανότητες<br>• Ικανότητα γραμματισμού<br>• Προσωπική, κοινωνική και μεταγνωστική ικανότητα<br>• Πολυγλωσσική ικανότητα<br>• Μαθηματική ικανότητα και ικανότητα στις θετικές επιστήμες, την τεχνολογία και τη μηχανική | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5<br><br>«Μπορεί να διαχειρίζεται και να επιβλέπει στο πλαίσιο συγκεκριμένης εργασίας ή διαδικασίας μάθησης, όπου μπορεί να συμβαίνουν και απρόβλεπτες αλλαγές. Μπορεί να αναθεωρεί και να αναπτύσσει τόσο την προσωπική του απόδοση όσο και άλλων ατόμων» |

| | |
|---|---|
| ΕΕΛ 1.2 | ΕΦΑΡΜΟΖΕΙ ΤΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ, ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ |
| | ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΕΡΓΑΣΙΕΣ<br>**1.2.1.** Προβαίνει σε ασφαλή διαμόρφωση εξοπλισμού και εφαρμογών του Οργανισμού (secure configuration)<br>**1.2.2.** Εφαρμόζει διαδικασίες και μηχανισμούς διαχείρισης, αυθεντικοποίησης και ελέγχου της πρόσβασης των χρηστών, στα πληροφοριακά συστήματα του Οργανισμού<br>**1.2.3.** Εφαρμόζει τεχνολογίες και λαμβάνει μέτρα ασφάλειας για την προστασία της δικτυακής υποδομής του Οργανισμού<br>**1.2.4.** Λαμβάνει μέτρα ασφάλειας και προστασίας από κακόβουλο-ιομορφικό λογισμικό και εγκαθιστά ενημερώσεις ασφάλειας (Security patches) για τα λειτουργικά συστήματα και τις εφαρμογές του Οργανισμού<br>**1.2.5.** Υλοποιεί μέτρα και διαδικασίες για την ασφαλή πραγματοποίηση απομακρυσμένης εργασίας από τους εργαζόμενους και την προστασία των κρίσιμων δεδομένων του Οργανισμού<br>**1.2.6.** Αντιμετωπίζει επιθέσεις στα πληροφοριακά συστήματα, δίκτυα και δεδομένα του Οργανισμού.<br>**1.2.7.** Εφαρμόζει μέτρα κρυπτογράφησης των κρίσιμων δεδομένων και πληροφοριών του Οργανισμού και υλοποιεί μηχανισμούς αποτροπής διαρροής τους<br>**1.2.8**. Διασφαλίζει τη διαθεσιμότητα των δεδομένων και πληροφοριών του Οργανισμού<br>**1.2.9.** Λαμβάνει μέτρα φυσικής ασφάλειας και περιβαλλοντικής προστασίας του υπολογιστικού και δικτυακού εξοπλισμού του Οργανισμού, καθώς και για την ασφαλή κατάργηση και καταστροφή, τόσο των φυσικών όσο και των ηλεκτρονικών αρχείων και εξοπλισμών |

ΚΡΙΤΗΡΙΑ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ

- Προβαίνει σε ασφαλή διαμόρφωση (secure configuration) εξοπλισμού και εφαρμογών του Οργανισμού, σε σταθμούς εργασίας (desktops, laptops), διακομιστές (servers), δικτυακές συσκευές (routers, switches, ασύρματα access points, firewalls), σε τακτική βάση, περιορίζοντας τη χρήση και εκτέλεση προγραμμάτων και υπηρεσιών στα πληροφοριακά συστήματα, λαμβάνοντας υπόψη τις βέλτιστες πρακτικές και τις οδηγίες ασφάλειας του εκάστοτε προμηθευτή/κατασκευαστή και τα διεθνή πρότυπα ασφάλειας πληροφοριών.
- Εφαρμόζει διαδικασίες και μηχανισμούς διαχείρισης, αυθεντικοποίησης και ελέγχου της πρόσβασης των χρηστών, στα πληροφοριακά συστήματα του Οργανισμού, εφαρμόζοντας την αρχή της ελάχιστης λειτουργικότητας (least functionality) και ρυθμίζοντας το σύνολο των συστημάτων, έτσι ώστε να παρέχουν μόνο τις λειτουργίες και υπηρεσίες που υποστηρίζουν την επιχειρησιακή αποστολή του Οργανισμού.
- Εφαρμόζει κατάλληλες τεχνολογίες και λαμβάνει τα απαραίτητα μέτρα ασφάλειας για την προστασία της δικτυακής υποδομής του Οργανισμού, εφαρμόζοντας και επικαιροποιώντας κατάλληλους δικτυακούς κανόνες επικοινωνίας, σε περιοδική βάση, χρησιμοποιώντας αποκλειστικά ασφαλή πρωτόκολλα και υπηρεσίες (π.χ. sftp, ssh, https, smbv3).
- Λαμβάνει κατάλληλα μέτρα ασφάλειας και προστασίας από κακόβουλο-ιομορφικό λογισμικό και εγκαθιστά, σε τακτικά χρονικά διαστήματα, τις τελευταίες απαραίτητες ενημερώσεις ασφάλειας (Security patches) για τα λειτουργικά συστήματα και τις εφαρμογές του Οργανισμού, σύμφωνα με την υπάρχουσα Πολιτική Ασφάλειας και Προστασίας από Κακόβουλο Λογισμικό.
- Αντιμετωπίζει επιθέσεις στα πληροφοριακά συστήματα, δίκτυα και δεδομένα του Οργανισμού εφαρμόζοντας τα προβλεπόμενα πρωτόκολλα και τα κατάλληλα μέτρα.
- Υλοποιεί τα απαραίτητα μέτρα και διαδικασίες για την ασφαλή πραγματοποίηση απομακρυσμένης εργασίας από τους εργαζόμενους και την προστασία των κρίσιμων δεδομένων του Οργανισμού, σύμφωνα με την Πολιτική Ασφάλειας Τηλεργασίας και Απομακρυσμένης Πρόσβασης και τις ειδικότερες οδηγίες της διοίκησης του Οργανισμού.
- Εφαρμόζει τα ενδεδειγμένα μέτρα κρυπτογράφησης των κρίσιμων δεδομένων και πληροφοριών του Οργανισμού, τόσο κατά την αποθήκευση όσο και κατά τη μετάδοσή τους, ώστε να διασφαλίζεται η εμπιστευτικότητα των δεδομένων και πληροφοριών, και υλοποιεί μηχανισμούς αποτροπής διαρροής τους (π.χ. περιορισμός/απαγόρευση χρήσης φορητών αποθηκευτικών μέσων).
- Διασφαλίζει τη διαθεσιμότητα των δεδομένων και πληροφοριών του Οργανισμού, εφαρμόζοντας, περιοδικά, τεχνολογίες και διαδικασίες λήψης αντιγράφων ασφάλειας (backup) και ασφαλούς φύλαξής τους.
- Λαμβάνει κατάλληλα μέτρα φυσικής ασφάλειας και περιβαλλοντικής προστασίας του υπολογιστικού και δικτυακού εξοπλισμού του Οργανισμού, καθώς και για την ασφαλή κατάργηση και καταστροφή, τόσο των φυσικών όσο και των ηλεκτρονικών αρχείων και εξοπλισμών, ακολουθώντας τα σχετικά προβλεπόμενα στην Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων του Οργανισμού.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

*Περιβάλλον και συνθήκες εργασίας:*

Επιχειρήσεις, Οργανισμοί, Υπηρεσίες κλπ. όπου υπάρχουν και χρησιμοποιούνται υπολογιστικά και πληροφοριακά συστήματα, καθώς και δικτυακός εξοπλισμός, Επιχειρήσεις και Οργανισμοί, που κατασκευάζουν, προωθούν - πωλούν και υποστηρίζουν προϊόντα ή υπηρεσίες πληροφορικής, Εμπορικές αντιπροσωπείες προϊόντων υπολογιστικών συστημάτων, επιχειρήσεις που παρέχουν υπηρεσίες υποστήριξης προς τρίτους ή/και παροχή συμβουλευτικών υπηρεσιών σε θέματα IT Security, Cyber security και Security as a service κτλ.

Δύναται να διαθέτει ανεξάρτητο χώρο-γραφείο μέσα στον Οργανισμό με τον απαραίτητο και αναγκαίο εξοπλισμό πληροφορικής για την εκτέλεση των καθηκόντων του.

*Μέσα/εργαλεία/υλικά:*

- Συνήθης εξοπλισμός γραφείου (Διαδίκτυο, Η/Υ, τηλεφωνική συσκευή και προσωπική διεύθυνση ηλεκτρονικής αλληλογραφίας για επικοινωνία και υποστήριξη (e-mail)).
- Λειτουργικά Συστήματα (Windows, Linux, Android κ.ά.) και πακέτα εφαρμογών/σουίτες γραφείου και βοηθητικά λογισμικά (Office, Libre Office, OpenOffice - Word, Excel, Internet, PowerPoint κλπ., Readers, Players, εργαλεία συμπίεσης - αποσυμπίεσης κλπ.).
- Ψηφιακά μέσα αποθήκευσης (USB, CD ή DVD).
- Τεχνικές και βοηθητικά προγράμματα/λογισμικά παρακολούθησης, βελτιστοποίησης, αναβάθμισης, διαχείρισης και συντήρησης.
- Εγχειρίδια και οδηγίες χρήσης και εγκατάστασης λογισμικών, εφαρμογών και εξειδικευμένων λογισμικών ασφάλειας πληροφοριών.

*Παραγόμενη υπηρεσία:*

Εφαρμογή μέτρων ασφάλειας στα πληροφοριακά συστήματα, στα δίκτυα και στις πληροφορίες του Οργανισμού.

*Μέθοδοι εφαρμογής και διαδικασίες:*

- Πολιτική Ασφάλειας πληροφοριακών συστημάτων και Προστασίας Δεδομένων και ειδικότερες Πολιτικές και Διαδικασίες.
- Ειδικότερες Πολιτικές, Πρότυπα, Διαδικασίες και Οδηγίες σχετιζόμενες με την Ασφάλεια Πληροφοριών (Security Policies, Standards, Procedures, and Guidelines).
- Διεθνή πρότυπα ασφάλειας πληροφοριών (όπως ISO/IEC 27001, 27002, ISO/IEC 29151, Control Objectives for Information Technology (CobIT), Common Criteria, NIST/SP 800-53, ENISA).
- Τεχνικά εγχειρίδια Κυβερνοασφάλειας (Cybersecurity-Handbooks) με βέλτιστες πρακτικές για την ασφάλεια, προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων.
- Λογισμικά/προγράμματα λήψης αντιγράφων ασφάλειας (backup).
- Διαδικασίες διαχείρισης και πολιτική ελέγχου της πρόσβασης.
- Εργαλεία πρόληψης ή αποτροπής απώλειας δεδομένων/πληροφοριών (DLP – Data Loss Prevention).
- Δικτυακά συστήματα ανίχνευσης και πρόληψης εισβολών (network intrusion detection /prevention systems).
- Πολιτική Διαχωρισμού Καθηκόντων (Segregation of Duties – SoD).
- Τεχνικές οδηγίες ασφαλούς καταστροφής δεδομένων/πληροφοριών/ψηφιακών μέσων.
- Προγράμματα ασφάλειας και προστασίας από κακόβουλο-ιομορφικό λογισμικό.
- Λογισμικά/εργαλεία κρυπτογράφησης.
- Πρωτόκολλα και μέτρα αντιμετώπισης κυβερνοεπιθέσεων.

ΓΕΝΙΚΕΣ ΓΝΩΣΕΙΣ

Ως ελάχιστες προαπαιτούμενες Γνώσεις, Δεξιότητες και Ικανότητες για την περαιτέρω επαγγελματική εκπαίδευση, κατάρτιση ή επαγγελματική δραστηριότητα είναι αυτές που αντιστοιχούν:

- στο επίπεδο 2 του Εθνικού και Ευρωπαϊκού Πλαισίου Προσόντων (ΕΠΠ) «Αποκτά βασικές γενικές γνώσεις, που σχετίζονται με ένα πεδίο εργασίας ή σπουδής, που του επιτρέπουν να αντιλαμβάνεται τις διαδικασίες εφαρμογής βασικών καθηκόντων και οδηγιών» για τις περιπτώσεις αποφοίτων ΕΠΑΣ, Γενικού Λυκείου και ΕΠΑΛ και
- στο επίπεδο 4 του Εθνικού και Ευρωπαϊκού Πλαισίου Προσόντων (ΕΠΠ) «Αποκτά ευρύ φάσμα θεωρητικών γνώσεων και ανάλυσης πληροφοριών που του επιτρέπουν να κατανοεί το πεδίο εργασίας ή σπουδής και να εφαρμόζει στοιχεία και διαδικασίες σε ένα γενικό πλαίσιο» για τις περιπτώσεις αποφοίτων ΙΕΚ και Μεταλυκειακού Έτους- Τάξης Μαθητείας.

| ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΓΝΩΣΕΙΣ | |
|---|---|
| • Ασφάλεια πληροφοριακών συστημάτων, δικτύων και πληροφοριών<br>• Βασικές γνώσεις, έννοιες και εντολές προγραμματισμού Η/Υ | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5: |

| | |
|---|---|
| • Γνώσεις διασύνδεσης, συνδεσμολογίας και αρχιτεκτονικής δικτύων και υπολογιστικών συστημάτων<br>• Αρχές συντήρησης και αναβάθμισης υλικού και λογισμικού<br>• Γνώση και υλοποίηση προτύπων ασφάλειας πληροφοριών (όπως ISO/IEC 27001, 27002, ISO/IEC 29151, Control Objectives for Information Technology (CobIT), Common Criteria, NIST/SP 800-53, ENISA)<br>• Πρωτόκολλα, τεχνολογίες και μηχανισμοί ταυτοποίησης και αυθεντικοποίησης<br>• Γνώση τεχνολογιών και λογισμικών που ανιχνεύουν την εγκατάσταση, εκτέλεση και μετάδοση κακόβουλου/ιομορφικού λογισμικού<br>• Αλγόριθμοι, πρωτόκολλα και λογισμικά κρυπτογράφησης και αποκρυπτογράφησης, ψευδωνυμοποιήσης και ανωνυμοποιήσης<br>• Γνώσεις αντιμετώπισης κυβερνοεπιθέσεων.<br>• Τεχνική ορολογία (ελληνική και αγγλική). | «Διαθέτει ευρείες, εξειδικευμένες, αντικειμενικές και θεωρητικές γνώσεις σε ένα πεδίο εργασίας ή σπουδής και έχει επίγνωση των ορίων των γνώσεων αυτών.» |
| ΕΙΔΙΚΕΣ ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΓΝΩΣΕΙΣ<br>Δεν υπάρχουν | |
| ΔΕΞΙΟΤΗΤΕΣ<br>• Χρήση προγραμμάτων, λογισμικών και λειτουργικών συστημάτων (προγράμματα εφαρμογών γραφείου, προγράμματα επεξεργασίας φωτογραφίας και εικόνων, προγράμματα διαχείρισης προσωπικών πληροφοριών, προγράμματα συμπίεσης/αποσυμπίεσης αρχείων, λογισμικά εφαρμογών, λογισμικά συστήματος, λειτουργικά συστήματα ανοικτού και κλειστού κώδικα κτλ.)<br>• Εφαρμογή προτύπων/ τεχνικών/ μεθοδολογιών ασφάλειας πληροφοριών και προστασίας δεδομένων<br>• Τήρηση και εφαρμογή εθνικών και διεθνών προτύπων ασφάλειας πληροφοριών<br>• Εφαρμογή και χρήση προτύπων, κανόνων και εργαλείων σύγχρονης και ασύγχρονης επικοινωνίας<br>• Χρήση εργαλείων και τεχνολογιών για τη δημιουργία, εποπτεία και έλεγχο αντιγράφων ασφάλειας<br>• Συγγραφή, σχεδιασμός και ανάπτυξη πολιτικών, διαδικασιών τεχνικών και εγχειρίδιων ασφάλειας πληροφοριακών συστημάτων, καθώς και κατάρτιση και προώθηση κατευθυντηρίων γραμμών<br>• Εφαρμογή εργαλείων πρόληψης ή αποτροπής απώλειας δεδομένων/πληροφοριών (DLP – Data Loss Prevention)<br>• Εφαρμογή λογισμικών/ προγραμμάτων λήψης αντιγράφων ασφάλειας (backup)<br>• Εφαρμογή μέτρων αντιμετώπισης κυβερνοεπιθέσεων | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5:<br>«Κατέχει ευρύ φάσμα γνωστικών και πρακτικών δεξιοτήτων που απαιτούνται για την εξεύρεση δημιουργικών λύσεων σε αφηρημένα προβλήματα.» |

| ΨΗΦΙΑΚΕΣ ΔΕΞΙΟΤΗΤΕΣ | Επίπεδο χρήστη | Κατηγορίες Ψηφιακών Δεξιοτήτων | | | | |
|---|---|---|---|---|---|---|
| | | Επεξεργασία Δεδομένων | Δημιουργία Περιεχομένου | Επικοινωνία | Επίλυση Προβλημάτων | Ασφάλεια |
| | Βασικός | - | - | - | - | - |
| | Ανεξάρτητος | - | ✓ | - | - | - |
| | Έμπειρος | ✓ | - | ✓ | ✓ | ✓ |

| | |
|---|---|
| ΙΚΑΝΟΤΗΤΕΣ<br>Βασικές Ικανότητες | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5 |

| | |
|---|---|
| • Ικανότητα γραμματισμού<br>• Μαθηματική ικανότητα και ικανότητα στις θετικές επιστήμες, την τεχνολογία και τη μηχανική<br>• Προσωπική, κοινωνική και μεταγνωστική ικανότητα<br>• Πολυγλωσσική ικανότητα. | «Μπορεί να διαχειρίζεται και να επιβλέπει στο πλαίσιο συγκεκριμένης εργασίας ή διαδικασίας μάθησης, όπου μπορεί να συμβαίνουν και απρόβλεπτες αλλαγές. Μπορεί να αναθεωρεί και να αναπτύσσει τόσο την προσωπική του απόδοση όσο και άλλων ατόμων» |

| | |
|---|---|
| ΕΕΛ 1.3 | ΕΛΕΓΧΕΙ ΤΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ, ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ |
| | ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΕΡΓΑΣΙΕΣ<br>**1.3.1.** Επιβλέπει, επιθεωρεί και ελέγχει την εφαρμογή των μέτρων ασφάλειας που έχουν προβλεφθεί στην Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων του Οργανισμού<br>**1.3.2.** Συλλέγει, συσχετίζει και παρακολουθεί τα αρχεία καταγραφής γεγονότων συστήματος και ενεργειών των χρηστών (system, event and application log files) στα κρίσιμα πληροφοριακά συστήματα<br>**1.3.3.** Υλοποιεί τεχνικούς ελέγχους αξιολόγησης των μέτρων ασφάλειας των πληροφοριακών συστημάτων του Οργανισμού<br>**1.3.4.** Διενεργεί έλεγχο ακεραιότητας και αξιοπιστίας των αντιγράφων ασφάλειας, καθώς και δοκιμή επαναφοράς δεδομένων (restoration)<br>**1.3.5.** Ελέγχει τις εφαρμογές και δικτυακές υπηρεσίες πριν την εγκατάσταση ή υλοποίησή τους<br>**1.3.6.** Ελέγχει και επιθεωρεί τα μέτρα φυσικής ασφάλειας και περιβαλλοντικής προστασίας του υπολογιστικού και δικτυακού εξοπλισμού του Οργανισμού |

ΚΡΙΤΗΡΙΑ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ

- Επιβλέπει, επιθεωρεί και ελέγχει, σε τακτά χρονικά διαστήματα, την εφαρμογή των μέτρων ασφάλειας που έχουν προβλεφθεί και καταγραφεί στην Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων του Οργανισμού, συντάσσοντας σχετική αναφορά (report) προς τη Διοίκηση του Οργανισμού περί των αποτελεσμάτων και ευρημάτων, με προτάσεις για βελτίωση της ασφάλειας, αν απαιτείται.
- Συλλέγει συστηματικά (σε πραγματικό χρόνο), συσχετίζει και παρακολουθεί, περιοδικά, με τη βοήθεια κατάλληλων εργαλείων/ πλατφορμών (π.χ. SIEM, Log monitoring tools), τα αρχεία καταγραφής γεγονότων συστήματος και ενεργειών (system, event and application log files) των χρηστών στα κρίσιμα πληροφοριακά συστήματα, για την έγκαιρη ανίχνευση κακόβουλης δραστηριότητας και την αποτελεσματική αντιμετώπιση περιστατικών παραβίασης της ασφάλειας πληροφοριακών συστημάτων, σύμφωνα με την εσωτερικά εφαρμοζόμενη διαδικασία συλλογής τους.
- Υλοποιεί, σε περιοδική βάση ή/και κατά την ανάπτυξη/ένταξη συστημάτων και εφαρμογών, τεχνικούς ελέγχους αξιολόγησης των μέτρων ασφάλειας των πληροφοριακών συστημάτων του Οργανισμού (Penetration tests, vulnerability assessment, security code reviews), εφαρμόζοντας εργαλεία ανίχνευσης αδυναμιών ασφάλειας πληροφοριών κάνοντας χρήση τεχνικών προσομοίωσης κακόβουλων επιθέσεων και προτείνοντας βελτιώσεις όπου απαιτείται.
- Διενεργεί, σε περιοδική βάση, έλεγχο ακεραιότητας και αξιοπιστίας των αντιγράφων ασφάλειας που λαμβάνονται, καθώς και δοκιμή επαναφοράς δεδομένων (restoration), κατ' ελάχιστο μία (1) φορά ετησίως, σύμφωνα με την εσωτερικά εφαρμοζόμενη πολιτική και διαδικασία λήψης και διαχείρισης αντιγράφων ασφάλειας (Backup).
- Ελέγχει επιμελώς τις εφαρμογές και δικτυακές υπηρεσίες πριν την εγκατάσταση ή/και υλοποίησή τους στον Οργανισμό, για τον έγκαιρο εντοπισμό τυχόν ευπαθειών ή κενών ασφάλειας, προτού αυτές μεταβούν σε λειτουργική φάση, λαμβάνοντας υπόψη τις βέλτιστες πρακτικές ή/και τις οδηγίες ασφάλειας του εκάστοτε προμηθευτή/κατασκευαστή.
- Ελέγχει και επιθεωρεί, τακτικά, τα μέτρα φυσικής ασφάλειας και περιβαλλοντικής προστασίας του υπολογιστικού και δικτυακού εξοπλισμού του Οργανισμού για τη διαπίστωση της εύρυθμης και ορθής λειτουργίας τους, σύμφωνα με τις ειδικότερες οδηγίες και κατευθύνσεις της διοίκησης του Οργανισμού.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

*Περιβάλλον και συνθήκες εργασίας:*

Επιχειρήσεις, Οργανισμοί, Υπηρεσίες κλπ. όπου υπάρχουν και χρησιμοποιούνται υπολογιστικά και πληροφοριακά συστήματα, καθώς και δικτυακός εξοπλισμός, Επιχειρήσεις και Οργανισμοί, που κατασκευάζουν, προωθούν - πωλούν και υποστηρίζουν προϊόντα ή υπηρεσίες

Πληροφορικής, Εμπορικές αντιπροσωπείες προϊόντων υπολογιστικών συστημάτων, επιχειρήσεις που παρέχουν υπηρεσίες υποστήριξης προς τρίτους ή/και παροχή συμβουλευτικών υπηρεσιών σε θέματα IT Security, Cyber security και Security as a service κτλ.

Δύναται να διαθέτει ανεξάρτητο χώρο-γραφείο μέσα στον Οργανισμό με τον απαραίτητο και αναγκαίο εξοπλισμό πληροφορικής για την εκτέλεση των καθηκόντων του.

*Μέσα/εργαλεία/υλικά:*

- Συνήθης εξοπλισμός γραφείου (Διαδίκτυο, Η/Υ, τηλεφωνική συσκευή και προσωπική διεύθυνση ηλεκτρονικής αλληλογραφίας για επικοινωνία και υποστήριξη (e-mail))
- Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων
- Λειτουργικά Συστήματα (Windows, Linux, Android κ.ά.) και πακέτα εφαρμογών/σουίτες γραφείου και βοηθητικά λογισμικά (Office, Libre Office, OpenOffice - Word, Excel, Internet, PowerPoint κλπ., Readers, Players, εργαλεία συμπίεσης - αποσυμπίεσης κλπ.)
- Τεχνικές και βοηθητικά προγράμματα/λογισμικά παρακολούθησης και εποπτείας
- Πρότυπα και φόρμες ελέγχου ασφάλειας πληροφοριακών συστημάτων (IT Security Audit Checklists)
- Εγχειρίδια και οδηγίες χρήσης και εγκατάστασης λογισμικών, εφαρμογών και εξειδικευμένων λογισμικών ασφάλειας πληροφοριών
- Τυποποιημένα έγγραφα (αναφορές, πρωτόκολλα κλπ.)
- Ψηφιακά μέσα αποθήκευσης (USB, CD ή DVD)
- Εργαλεία/λογισμικά/πλατφόρμες για συλλογή, συσχέτιση και παρακολούθηση των αρχείων καταγραφής γεγονότων συστήματος και ενεργειών των χρηστών στα πληροφοριακά συστήματα
- Εργαλεία/λογισμικά/προγράμματα για διενέργεια τεχνικών ελέγχων αξιολόγησης (Penetration tests, vulnerability assessment, security code reviews) μέτρων ασφάλειας πληροφοριακών συστημάτων, εφαρμογών και δικτυακών υπηρεσιών
- Εργαλεία/λογισμικά/προγράμματα για δοκιμή επαναφοράς δεδομένων (restoration) από αντίγραφα ασφάλειας
- Έντυπα επιθεώρησης, παρακολούθησης και ελέγχου των μέτρων ασφάλειας πληροφοριακών συστημάτων

*Παραγόμενη υπηρεσία:*

Έλεγχος των μέτρων ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων του Οργανισμού

*Μέθοδοι εφαρμογής και διαδικασίες:*

- Ειδικότερες Πολιτικές, Πρότυπα, Διαδικασίες και Οδηγίες σχετιζόμενες με την Ασφάλεια Πληροφοριών (Security Policies, Standards, Procedures, and Guidelines)
- Διεθνή πρότυπα ασφάλειας πληροφοριών (όπως ISO/IEC 27001, 27002, ISO/IEC 29151, Control Objectives for Information Technology (CobIT), Common Criteria, NIST/SP 800-53, ENISA)
- Τεχνικά εγχειρίδια Κυβερνοασφάλειας (Cybersecurity-Handbooks) με βέλτιστες πρακτικές για την ασφάλεια, προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων
- Ταξινομημένη και καταγεγραμμένη λίστα εργασιών, σύμφωνα με τη σπουδαιότητά τους
- Πολιτική συλλογής, συσχέτισης και παρακολούθησης των αρχείων καταγραφής γεγονότων συστήματος και ενεργειών των χρηστών στα πληροφοριακά συστήματα
- Πολιτική και διαδικασίες διενέργειας τεχνικών ελέγχων αξιολόγησης μέτρων ασφάλειας πληροφοριακών συστημάτων, εφαρμογών και δικτυακών υπηρεσιών
- Πολιτική επιθεώρησης, παρακολούθησης και ελέγχου των μέτρων ασφάλειας πληροφοριακών συστημάτων
- Τυποποιημένες διαδικασίες καταγραφής επιθεωρήσεων και ελέγχων.

ΓΕΝΙΚΕΣ ΓΝΩΣΕΙΣ

Ως ελάχιστες προαπαιτούμενες Γνώσεις, Δεξιότητες και Ικανότητες για την περαιτέρω επαγγελματική εκπαίδευση, κατάρτιση ή επαγγελματική δραστηριότητα είναι αυτές που αντιστοιχούν:

- στο επίπεδο 2 του Εθνικού και Ευρωπαϊκού Πλαισίου Προσόντων (ΕΠΠ) «Αποκτά βασικές γενικές γνώσεις, που σχετίζονται με ένα πεδίο εργασίας ή σπουδής, που του επιτρέπουν να αντιλαμβάνεται τις διαδικασίες εφαρμογής βασικών καθηκόντων και οδηγιών» για τις περιπτώσεις αποφοίτων ΕΠΑΣ, Γενικού Λυκείου και ΕΠΑΛ και
- στο επίπεδο 4 του Εθνικού και Ευρωπαϊκού Πλαισίου Προσόντων (ΕΠΠ) «Αποκτά ευρύ φάσμα θεωρητικών γνώσεων και ανάλυσης πληροφοριών που του επιτρέπουν να κατανοεί το πεδίο εργασίας ή σπουδής και να εφαρμόζει στοιχεία και διαδικασίες σε ένα γενικό πλαίσιο» για τις περιπτώσεις αποφοίτων ΙΕΚ και Μεταλυκειακού Έτους- Τάξης Μαθητείας.

ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΓΝΩΣΕΙΣ

- Ασφάλεια πληροφοριακών συστημάτων, δικτύων και πληροφοριών
- Βασικές γνώσεις, έννοιες και εντολές προγραμματισμού Η/Υ

| | |
|---|---|
| • Διαδικασίες, τεχνικές, εργαλεία και μεθοδολογίες ελέγχου ασφάλειας πληροφορικών συστημάτων (IT Security Audit)<br>• Γνώσεις για τεχνικούς ελέγχους αξιολόγησης (Penetration tests, vulnerability assessment, security code reviews) της επάρκειας, καταλληλόλητας και αποτελεσματικότητας μέτρων ασφάλειας πληροφοριακών συστημάτων<br>• Συστήματα βιντεοεπιτήρησης και κλειστού κυκλώματος τηλεόρασης (CCTV-Closed Circuit TV Systems)<br>• Τεχνική ορολογία (ελληνική και αγγλική). | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5:<br>«Διαθέτει ευρείες, εξειδικευμένες, αντικειμενικές και θεωρητικές γνώσεις σε ένα πεδίο εργασίας ή σπουδής και έχει επίγνωση των ορίων των γνώσεων αυτών.» |
| ΕΙΔΙΚΕΣ ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΓΝΩΣΕΙΣ<br><br>Δεν υπάρχουν | |
| ΔΕΞΙΟΤΗΤΕΣ<br><br>• Χρήση προγραμμάτων, λογισμικών και λειτουργικών συστημάτων. (προγράμματα εφαρμογών γραφείου, προγράμματα επεξεργασίας φωτογραφίας και εικόνων, προγράμματα διαχείρισης προσωπικών πληροφοριών, προγράμματα συμπίεσης/αποσυμπίεσης αρχείων, λογισμικά εφαρμογών, λογισμικά συστήματος, λειτουργικά συστήματα ανοικτού και κλειστού κώδικα κτλ.)<br>• Χρήση εργαλείων για τεχνικούς ελέγχους ασφάλειας πληροφοριών<br>• Τήρηση και εφαρμογή εθνικών και διεθνών προτύπων ασφάλειας πληροφοριών<br>• Εφαρμογή και χρήση προτύπων, κανόνων και εργαλείων σύγχρονης και ασύγχρονης επικοινωνίας<br>• Χρήση εργαλείων και τεχνολογιών για εποπτεία και έλεγχο αντιγράφων ασφάλειας. | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5:<br>«Κατέχει ευρύ φάσμα γνωστικών και πρακτικών δεξιοτήτων που απαιτούνται για την εξεύρεση δημιουργικών λύσεων σε αφηρημένα προβλήματα.» |

| ΨΗΦΙΑΚΕΣ ΔΕΞΙΟΤΗΤΕΣ | Επίπεδο χρήστη | Κατηγορίες Ψηφιακών Δεξιοτήτων | | | | |
|---|---|---|---|---|---|---|
| | | Επεξεργασία Δεδομένων | Δημιουργία Περιεχομένου | Επικοινωνία | Επίλυση Προβλημάτων | Ασφάλεια |
| | Βασικός | - | - | - | - | - |
| | Ανεξάρτητος | - | ✓ | - | - | - |
| | Έμπειρος | ✓ | - | ✓ | ✓ | ✓ |

| | |
|---|---|
| ΙΚΑΝΟΤΗΤΕΣ<br><br>Βασικές Ικανότητες<br><br>• Ικανότητα γραμματισμού<br>• Μαθηματική ικανότητα και ικανότητα στις θετικές επιστήμες, την τεχνολογία και τη μηχανική<br>• Προσωπική, κοινωνική και μεταγνωστική ικανότητα<br>• Πολυγλωσσική ικανότητα | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5<br><br>«Μπορεί να διαχειρίζεται και να επιβλέπει στο πλαίσιο συγκεκριμένης εργασίας ή διαδικασίας μάθησης, όπου μπορεί να συμβαίνουν και απρόβλεπτες αλλαγές. Μπορεί να αναθεωρεί και να αναπτύσσει τόσο την προσωπική του απόδοση όσο και άλλων ατόμων» |

| | |
|---|---|
| ΚΕΛ 2 | ΕΝΗΜΕΡΩΝΕΙ ΚΑΙ ΥΠΟΣΤΗΡΙΖΕΙ ΤΟΥΣ ΧΡΗΣΤΕΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΤΗ ΔΙΟΙΚΗΣΗ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ ΓΙΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ |
| ΕΕΛ 2.1 | ΕΝΗΜΕΡΩΝΕΙ ΤΟΥΣ ΧΡΗΣΤΕΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΤΗ ΔΙΟΙΚΗΣΗ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ ΓΙΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ<br><br>ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΕΡΓΑΣΙΕΣ<br><br>**2.1.1.** Συμβουλεύει, ενημερώνει και ευαισθητοποιεί τους χρήστες και τη Διοίκηση του Οργανισμού, σε θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων<br><br>**2.1.2.** Προετοιμάζει το προσωπικό του Οργανισμού για τις απαραίτητες ενέργειες και τρόπους αντίδρασης σε ενδεχόμενο περιστατικό ασφάλειας και παραβίασης προσωπικών δεδομένων<br><br>**2.1.3**.Τηρεί αρχείο-κατάλογο νομοθετικών κειμένων, κανονισμών κτλ. που σχετίζονται με την ασφάλεια πληροφοριακών συστημάτων, την προστασία προσωπικών δεδομένων και την προστασία δικαιωμάτων χρήσης λογισμικού. |

ΚΡΙΤΗΡΙΑ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ

- Συμβουλεύει, ενημερώνει και ευαισθητοποιεί, σε τακτά διαστήματα, τους χρήστες υπολογιστικών συστημάτων και τη Διοίκηση του Οργανισμού σε θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων, αξιοποιώντας κάθε πρόσφορο μέσο/τεχνική ενημέρωσης (σεμινάρια, φυλλάδια, γραπτά μηνύματα κτλ.), σε συνεργασία με τον Υπεύθυνο Ασφάλειας Πληροφοριών (CISO) και τον Υπεύθυνο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (DPO) του Οργανισμού, εφόσον υπάρχουν.
- Προετοιμάζει το προσωπικό του Οργανισμού για τις απαραίτητες ενέργειες και τρόπους αντίδρασης σε ενδεχόμενο περιστατικό ασφάλειας και παραβίασης προσωπικών δεδομένων, σύμφωνα με το πλάνο αντιμετώπισης και διαχείρισης περιστατικών ασφάλειας, καθώς και ανάκτησης δεδομένων, λειτουργικότητας και επιχειρησιακής συνέχειας, διενεργώντας κατάλληλα προσαρμοσμένες πρακτικές ασκήσεις προσομοίωσης συμβάντων και περιστατικών ασφάλειας.
- Τηρεί σχετικό αρχείο-κατάλογο επικαιροποιημένων νομοθετικών κειμένων, κανονισμών κτλ. που σχετίζονται με την ασφάλεια πληροφοριακών συστημάτων, την προστασία προσωπικών δεδομένων και την προστασία δικαιωμάτων χρήσης λογισμικού, παρακολουθώντας συστηματικά τις σχετικές νομοθετικές εξελίξεις.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

*Περιβάλλον και συνθήκες εργασίας*

Επιχειρήσεις, Οργανισμοί, Υπηρεσίες κλπ. όπου υπάρχουν και χρησιμοποιούνται υπολογιστικά και πληροφοριακά συστήματα, καθώς και δικτυακός εξοπλισμός, Επιχειρήσεις και Οργανισμοί, που κατασκευάζουν, προωθούν - πωλούν και υποστηρίζουν προϊόντα ή υπηρεσίες Πληροφορικής, Εμπορικές αντιπροσωπείες προϊόντων υπολογιστικών συστημάτων, επιχειρήσεις που παρέχουν υπηρεσίες υποστήριξης προς τρίτους ή/και παροχή συμβουλευτικών υπηρεσιών σε θέματα IT Security, Cyber security και Security as a service κτλ.

Δύναται να διαθέτει ανεξάρτητο χώρο-γραφείο μέσα στον Οργανισμό με τον απαραίτητο και αναγκαίο εξοπλισμό πληροφορικής για την εκτέλεση των καθηκόντων του.

*Μέσα/εργαλεία/υλικά:*

- Συνήθης εξοπλισμός γραφείου (Διαδίκτυο, Η/Υ, τηλεφωνική συσκευή και προσωπική διεύθυνση ηλεκτρονικής αλληλογραφίας για επικοινωνία και υποστήριξη (e-mail))
- Ψηφιακά μέσα αποθήκευσης (USB, CD ή DVD)
- Εκπαιδευτικό υλικό (φυλλάδια, βίντεο κτλ.) σχετικό με θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων
- Σενάρια/μελέτες περίπτωσης/πρακτικές ασκήσεις προσομοίωσης συμβάντων και περιστατικών ασφάλειας

*Παραγόμενη υπηρεσία:*

Ενημέρωση των χρηστών και της διοίκησης του Οργανισμού, σε θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων.

*Μέθοδοι εφαρμογής και διαδικασίες:*

- Διεθνή πρότυπα ασφάλειας πληροφοριών (όπως ISO/IEC 27001, 27002, ISO/IEC 29151, Control Objectives for Information Technology (CobIT), Common Criteria, NIST/SP 800-53, ENISA)
- Διεθνή πρότυπα για αντιμετώπιση, ανταπόκριση και διαχείριση περιστατικών ασφάλειας, ανάκτησης δεδομένων και επιχειρησιακής συνέχειας (όπως ISO/IEC 22301, ISO/IEC 27001 κτλ)
- Τεχνικά εγχειρίδια Κυβερνοασφάλειας (Cybersecurity-Handbooks) με βέλτιστες πρακτικές για την ασφάλεια, προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων
- Φάκελος με το ισχύον θεσμικό και κανονιστικό πλαίσιο (Νόμος 4624/2019 [Εφαρμογή GDPR], Νόμος 4577/2018 [Εφαρμογή Οδηγίας NIS]) για τα περιστατικά ασφάλειας και διαρροής δεδομένων και υποχρεώσεις - απαιτήσεις που απορρέουν από αυτό
- Πολιτική εκπαίδευσης, ενημέρωσης και ευαισθητοποίησης υπαλλήλων/εργαζομένων σε θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων
- Νομοθετικό και κανονιστικό πλαίσιο που σχετίζεται με την ασφάλεια πληροφοριακών συστημάτων, την προστασία προσωπικών δεδομένων και την νομοθεσία περί προστασίας δικαιωμάτων χρήσης λογισμικού
- Σχέδιο/πλάνο αντιμετώπισης και διαχείρισης περιστατικών ασφάλειας
- Σχέδιο/πλάνο επιχειρησιακής συνέχειας (Business Continuity Plan) και ανάκαμψης από καταστροφή (Disaster Recovery Plan), καθώς και ανάκτησης δεδομένων & λειτουργικότητας.

ΓΕΝΙΚΕΣ ΓΝΩΣΕΙΣ

Ως ελάχιστες προαπαιτούμενες Γνώσεις, Δεξιότητες και Ικανότητες για την περαιτέρω επαγγελματική εκπαίδευση, κατάρτιση ή επαγγελματική δραστηριότητα είναι αυτές που αντιστοιχούν:

- στο επίπεδο 2 του Εθνικού και Ευρωπαϊκού Πλαισίου Προσόντων (ΕΠΠ) «Αποκτά βασικές γενικές γνώσεις, που σχετίζονται με ένα πεδίο εργασίας ή σπουδής, που του επιτρέπουν να αντιλαμβάνεται τις διαδικασίες εφαρμογής βασικών καθηκόντων και οδηγιών» για τις περιπτώσεις αποφοίτων ΕΠΑΣ, Γενικού Λυκείου και ΕΠΑΛ και
- στο επίπεδο 4 του Εθνικού και Ευρωπαϊκού Πλαισίου Προσόντων (ΕΠΠ) «Αποκτά ευρύ φάσμα θεωρητικών γνώσεων και ανάλυσης πληροφοριών που του επιτρέπουν να κατανοεί το πεδίο εργασίας ή σπουδής και να εφαρμόζει στοιχεία και διαδικασίες σε ένα γενικό πλαίσιο» για τις περιπτώσεις αποφοίτων ΙΕΚ και Μεταλυκειακού Έτους- Τάξης Μαθητείας.

| | |
|---|---|
| ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΓΝΩΣΕΙΣ<br>• Ασφάλεια πληροφοριακών συστημάτων, δικτύων και πληροφοριών<br>• Τεχνικές/διαδικασίες/πλατφόρμες εκπαίδευσης, ενημέρωσης και ευαισθητοποίησης υπαλλήλων/εργαζομένων σε βασικά θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων<br>• Γνώσεις και εργαλεία για διενέργεια πρακτικών ασκήσεων προσομοίωσης συμβάντων και περιστατικών ασφάλειας<br>• Νομοθετικό και κανονιστικό πλαίσιο που σχετίζεται με την ασφάλεια πληροφοριακών συστημάτων, την προστασία προσωπικών δεδομένων και τη νομοθεσία περί προστασίας δικαιωμάτων χρήσης λογισμικού. | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5:<br>«Διαθέτει ευρείες, εξειδικευμένες, αντικειμενικές και θεωρητικές γνώσεις σε ένα πεδίο εργασίας ή σπουδής και έχει επίγνωση των ορίων των γνώσεων αυτών.» |
| ΕΙΔΙΚΕΣ ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΓΝΩΣΕΙΣ<br>Δεν υπάρχουν | |
| ΔΕΞΙΟΤΗΤΕΣ<br>• Εφαρμογή τεχνικών εκπαίδευσης ενηλίκων<br>• Εφαρμογή και χρήση προτύπων, κανόνων και εργαλείων σύγχρονης και ασύγχρονης επικοινωνίας.<br>• Διαμόρφωση υλικού ενημέρωσης (σεμινάρια, φυλλάδια, γραπτά μηνύματα κτλ.)<br>• Αρχειοθέτηση νομοθετικών κειμένων. κανονισμών σε θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων. | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5:<br>«Κατέχει ευρύ φάσμα γνωστικών και πρακτικών δεξιοτήτων που απαιτούνται για την εξεύρεση δημιουργικών λύσεων σε αφηρημένα προβλήματα.» |

| ΨΗΦΙΑΚΕΣ ΔΕΞΙΟΤΗΤΕΣ | Επίπεδο χρήστη | Κατηγορίες Ψηφιακών Δεξιοτήτων | | | | |
|---|---|---|---|---|---|---|
| | | Επεξεργασία Δεδομένων | Δημιουργία Περιεχομένου | Επικοινωνία | Επίλυση Προβλημάτων | Ασφάλεια |
| | Βασικός | - | - | - | - | - |
| | Ανεξάρτητος | - | ✓ | - | - | - |
| | Έμπειρος | ✓ | - | ✓ | ✓ | ✓ |

| ΙΚΑΝΟΤΗΤΕΣ | |
|---|---|
| Βασικές Ικανότητες<br>• Ικανότητα γραμματισμού<br>• Μαθηματική ικανότητα και ικανότητα στις θετικές επιστήμες, την τεχνολογία και τη μηχανική<br>• Προσωπική, κοινωνική και μεταγνωστική ικανότητα<br>• Πολυγλωσσική ικανότητα | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5<br>«Μπορεί να διαχειρίζεται και να επιβλέπει στο πλαίσιο συγκεκριμένης εργασίας ή διαδικασίας μάθησης, όπου μπορεί να συμβαίνουν και απρόβλεπτες αλλαγές. Μπορεί να αναθεωρεί και να αναπτύσσει τόσο την προσωπική του απόδοση όσο και άλλων ατόμων» |

| | |
|---|---|
| ΕΕΛ 2.2 | ΥΠΟΣΤΗΡΙΖΕΙ ΤΟΥΣ ΧΡΗΣΤΕΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΤΗ ΔΙΟΙΚΗΣΗ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ ΣΕ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ |
| | ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΕΡΓΑΣΙΕΣ<br>**2.2.1.** Καθοδηγεί και υποστηρίζει τους χρήστες των πληροφοριακών συστημάτων και τη διοίκηση του Οργανισμού σε θέματα ασφάλειας που ανακύπτουν<br>**2.2.2.** Παραλαμβάνει και καταγράφει αναφορές των χρηστών για θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων<br>**2.2.3.** Εντοπίζει, διερευνά και επιλύει θέματα ασφάλειας πληροφοριών και δυσλειτουργίες των πληροφοριακών συστημάτων που ανακύπτουν από την εφαρμογή των μέτρων ασφάλειας<br>**2.2.4.** Καταγράφει και τεκμηριώνει τις λειτουργίες υποστήριξης που εκτελεί. |

ΚΡΙΤΗΡΙΑ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ

- Καθοδηγεί και υποστηρίζει τεχνικά τους χρήστες των πληροφοριακών συστημάτων και τη διοίκηση του Οργανισμού σε θέματα ασφάλειας που ανακύπτουν, με βάση τη σχετική νομοθεσία και την Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων του Οργανισμού.
- Παραλαμβάνει, τηλεφωνικά ή μέσω διαδικτύου, και καταγράφει τις αναφορές των χρηστών για ανακύπτοντα θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων, ιεραρχώντας αυτές ανάλογα με τη σπουδαιότητά τους.
- Εντοπίζει, διερευνά με επιμέλεια και επιλύει θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων και δυσλειτουργίες των πληροφοριακών συστημάτων, είτε ύστερα από αναφορές που λαμβάνει είτε όταν αυτά ανακύπτουν από την εφαρμογή και υλοποίηση των μέτρων ασφάλειας
- Καταγράφει αναλυτικά και τεκμηριώνει εγγράφως τις λειτουργίες υποστήριξης που εκτελεί, σύμφωνα με τους κανόνες και τις διαδικασίες διαχείρισης και υποστήριξης και τις ειδικότερες οδηγίες του Οργανισμού.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

*Περιβάλλον και συνθήκες εργασίας:*

Επιχειρήσεις, Οργανισμοί, Υπηρεσίες κλπ. όπου υπάρχουν και χρησιμοποιούνται υπολογιστικά και πληροφοριακά συστήματα, καθώς και δικτυακός εξοπλισμός, Επιχειρήσεις και Οργανισμοί, που κατασκευάζουν, προωθούν - πωλούν και υποστηρίζουν προϊόντα ή υπηρεσίες Πληροφορικής, Εμπορικές αντιπροσωπείες προϊόντων υπολογιστικών συστημάτων, επιχειρήσεις που παρέχουν υπηρεσίες υποστήριξης προς τρίτους ή/και παροχή συμβουλευτικών υπηρεσιών σε θέματα IT Security, Cyber security και Security as a service κτλ.

Δύναται να διαθέτει ανεξάρτητο χώρο-γραφείο μέσα στον Οργανισμό με τον απαραίτητο και αναγκαίο εξοπλισμό πληροφορικής για την εκτέλεση των καθηκόντων του/ης

*Μέσα/εργαλεία/υλικά:*

- Συνήθης εξοπλισμός γραφείου (Διαδίκτυο, Η/Υ, τηλεφωνική συσκευή και προσωπική διεύθυνση ηλεκτρονικής αλληλογραφίας για επικοινωνία και υποστήριξη (e-mail))
- Κανόνες ιεράρχησης βλαβών/δυσλειτουργιών θεμάτων ασφάλειας (χρόνος επίλυσης, πιθανή επίδραση σε άλλες λειτουργικές διαδικασίες, κ.ά.)
- Έντυπα καταγραφής λειτουργιών υποστήριξης
- Κεντρικό πληροφοριακό σύστημα καταγραφής και διαχείρισης συμβάντων ασφάλειας πληροφοριών
- Συστήμα εφαρμογής, καταχώρησης και παρακολούθησης αιτημάτων χρηστών των υπολογιστικών συστημάτων

*Παραγόμενη υπηρεσία:*

Υποστήριξη των χρηστών των πληροφοριακών συστημάτων σε ανακύπτοντα θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων

*Μέθοδοι εφαρμογής και διαδικασίες:*

- Διεθνή πρότυπα ασφάλειας πληροφοριών (όπως ISO/IEC 27001, 27002, ISO/IEC 29151, Control Objectives for Information Technology (CobIT), Common Criteria, NIST/SP 800-53, ENISA).
- Τεχνικά εγχειρίδια Κυβερνοασφάλειας (Cybersecurity-Handbooks) με βέλτιστες πρακτικές για την ασφάλεια, προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων
- Τυποποιημένα πρωτόκολλα διαδικασιών συντήρησης
- Ταξινομημένη και καταγεγραμμένη λίστα εργασιών, σύμφωνα με την σπουδαιότητά τους
- Καταγραφή προβλεπόμενων χρόνων επίλυσης κάθε προβλήματος, σε αρχείο

- Τυποποιημένα πρωτόκολλα διαδικασιών επίλυσης βλαβών/δυσλειτουργιών

ΓΕΝΙΚΕΣ ΓΝΩΣΕΙΣ

Ως ελάχιστες προαπαιτούμενες Γνώσεις, Δεξιότητες και Ικανότητες για την περαιτέρω επαγγελματική εκπαίδευση, κατάρτιση ή επαγγελματική δραστηριότητα είναι αυτές που αντιστοιχούν:

- στο επίπεδο 2 του Εθνικού και Ευρωπαϊκού Πλαισίου Προσόντων (ΕΠΠ) «Αποκτά βασικές γενικές γνώσεις, που σχετίζονται με ένα πεδίο εργασίας ή σπουδής, που του επιτρέπουν να αντιλαμβάνεται τις διαδικασίες εφαρμογής βασικών καθηκόντων και οδηγιών» για τις περιπτώσεις αποφοίτων ΕΠΑΣ, Γενικού Λυκείου και ΕΠΑΛ και
- στο επίπεδο 4 του Εθνικού και Ευρωπαϊκού Πλαισίου Προσόντων (ΕΠΠ) «Αποκτά ευρύ φάσμα θεωρητικών γνώσεων και ανάλυσης πληροφοριών που του επιτρέπουν να κατανοεί το πεδίο εργασίας ή σπουδής και να εφαρμόζει στοιχεία και διαδικασίες σε ένα γενικό πλαίσιο» για τις περιπτώσεις αποφοίτων ΙΕΚ και Μεταλυκειακού Έτους- Τάξης Μαθητείας.

| ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΓΝΩΣΕΙΣ | |
|---|---|
| • Ασφάλεια πληροφοριακών συστημάτων, δικτύων και πληροφοριών<br>• Γνώσεις αρχιτεκτονικής και συνδεσμολογίας δικτύων και υπολογιστικών συστημάτων<br>• Γνώσεις εντοπισμού και εφαρμογής ενημερώσεων και ελάχιστων προδιαγραφών ασφάλειας υπολογιστικών συστημάτων, λογισμικών και εφαρμογών<br>• Τεχνική ορολογία (ελληνική και αγγλική). | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5:<br>«Διαθέτει ευρείες, εξειδικευμένες, αντικειμενικές και θεωρητικές γνώσεις σε ένα πεδίο εργασίας ή σπουδής και έχει επίγνωση των ορίων των γνώσεων αυτών.» |
| ΕΙΔΙΚΕΣ ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΓΝΩΣΕΙΣ<br>Δεν υπάρχουν | |
| ΔΕΞΙΟΤΗΤΕΣ<br>• Χρήση προγραμμάτων, λογισμικών και λειτουργικών συστημάτων. (προγράμματα εφαρμογών γραφείου, προγράμματα επεξεργασίας φωτογραφίας και εικόνων, προγράμματα διαχείρισης προσωπικών πληροφοριών, προγράμματα συμπίεσης/αποσυμπίεσης αρχείων, λογισμικά εφαρμογών, λογισμικά συστήματος, λειτουργικά συστήματα ανοικτού και κλειστού κώδικα κτλ.)<br>• Τήρηση και εφαρμογή εθνικών και διεθνών προτύπων ασφάλειας πληροφοριών<br>• Εφαρμογή και χρήση προτύπων, κανόνων και εργαλείων σύγχρονης και ασύγχρονης επικοινωνίας. | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5:<br>«Κατέχει ευρύ φάσμα γνωστικών και πρακτικών δεξιοτήτων που απαιτούνται για την εξεύρεση δημιουργικών λύσεων σε αφηρημένα προβλήματα.» |

| ΨΗΦΙΑΚΕΣ ΔΕΞΙΟΤΗΤΕΣ | Επίπεδο χρήστη | Κατηγορίες Ψηφιακών Δεξιοτήτων | | | | |
|---|---|---|---|---|---|---|
| | | Επεξεργασία Δεδομένων | Δημιουργία Περιεχομένου | Επικοινωνία | Επίλυση Προβλημάτων | Ασφάλεια |
| | Βασικός | - | - | - | - | - |
| | Ανεξάρτητος | - | ✓ | - | - | - |
| | Έμπειρος | ✓ | - | ✓ | ✓ | ✓ |

| ΙΚΑΝΟΤΗΤΕΣ | |
|---|---|
| Βασικές Ικανότητες<br>• Ικανότητα γραμματισμού<br>• Μαθηματική ικανότητα και ικανότητα στις θετικές επιστήμες, την τεχνολογία και τη μηχανική<br>• Προσωπική, κοινωνική και μεταγνωστική ικανότητα | Αντιστοίχιση με το Εθνικό Πλαίσιο Προσόντων – Επίπεδο 5<br>«Μπορεί να διαχειρίζεται και να επιβλέπει στο πλαίσιο συγκεκριμένης εργασίας ή διαδικασίας μάθησης, όπου μπορεί να συμβαίνουν και απρόβλεπτες αλλαγές. Μπορεί να αναθεωρεί και να αναπτύσσει τόσο την προσωπική του απόδοση όσο και άλλων ατόμων» |

| | |
|---|---|
| • Πολυγλωσσική ικανότητα | |

| ΤΑΞΙΝΟΜΗΣΗ ΓΝΩΣΕΩΝ ΔΕΞΙΟΤΗΤΩΝ & ΙΚΑΝΟΤΗΤΩΝ ΣΕ ΕΠΙΠΕΔΟ ISCED[10] | |
|---|---|
| ISCED | ΕΠΙΠΕΔΟ 4 |
| ΠΑΡΑΤΗΡΗΣΕΙΣ | - |

[10] International Standard Classification of Education

ΕΝΟΤΗΤΑ Δ

# ΥΦΙΣΤΑΜΕΝΕΣ ΚΑΙ ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΔΙΑΔΡΟΜΕΣ ΓΙΑ ΤΗΝ ΑΠΟΚΤΗΣΗ ΤΩΝ ΑΠΑΙΤΟΥΜΕΝΩΝ ΠΡΟΣΟΝΤΩΝ

## ΕΝΟΤΗΤΑ Δ: «Υφιστάμενες και προτεινόμενες διαδρομές για την απόκτηση των απαιτούμενων προσόντων»

### ΥΦΙΣΤΑΜΕΝΕΣ ΔΙΑΔΡΟΜΕΣ

Οι υφιστάμενες εκπαιδευτικές διαδρομές είναι αυτές που προσδιορίζονται από νομοθετικές ρυθμίσεις, οι οποίες είναι σε ισχύ και περιγράφουν τις προϋποθέσεις για την απόκτηση επαγγελματικών αδειών και επαγγελματικών δικαιωμάτων για ένα συγκεκριμένο επάγγελμα.

Για το παρόν επαγγελματικό περίγραμμα δεν απαιτείται άδεια άσκησης επαγγέλματος.

### ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΔΙΑΔΡΟΜΕΣ

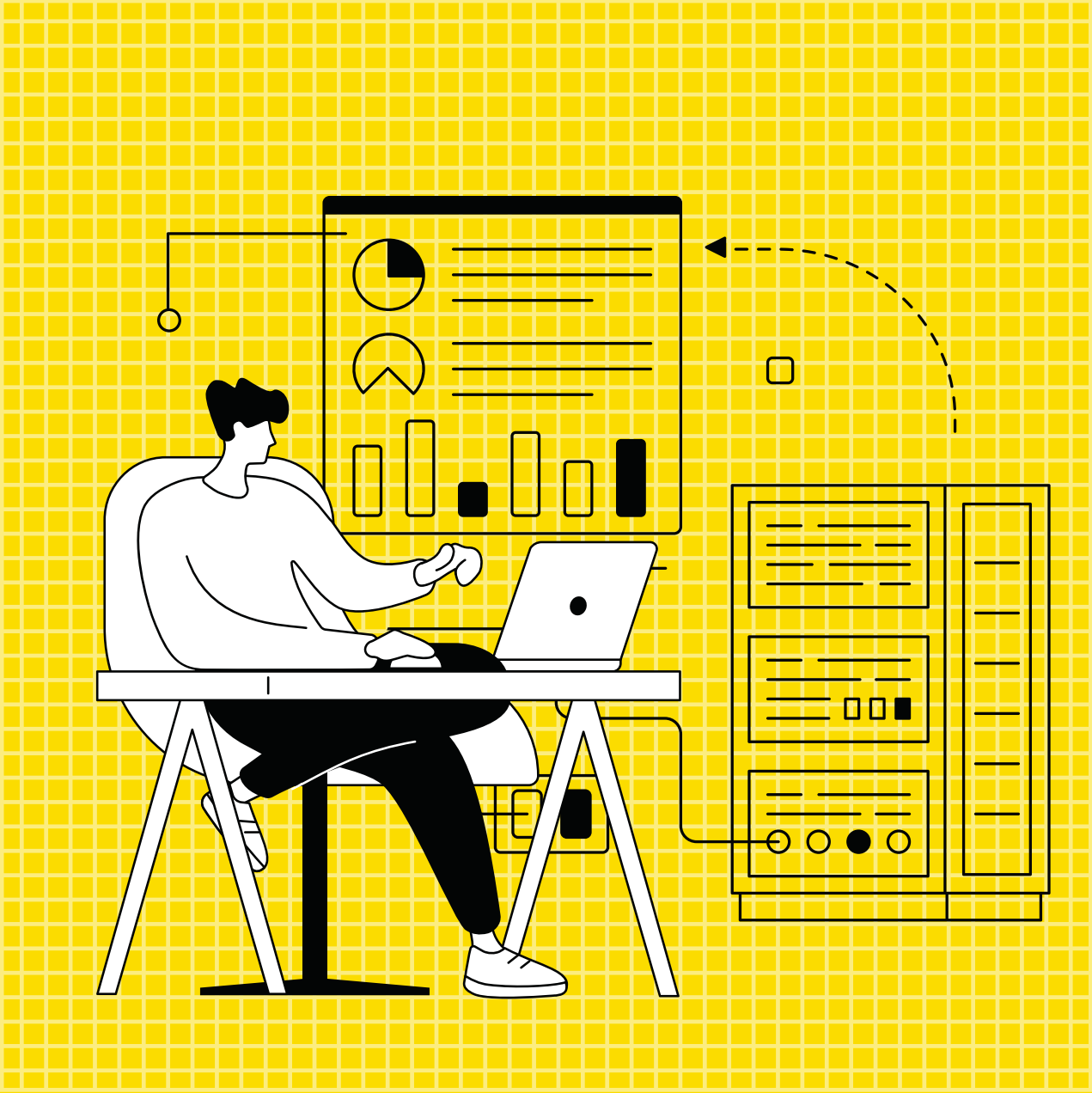
Στον παρακάτω πίνακα παρουσιάζονται οι διαδρομές μάθησης για το επάγγελμα του/της Τεχνικού ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist)

Οι παρακάτω διαδρομές δείχνουν (με βάση τη σειρά που αναφέρονται) τις εναλλακτικές επιλογές ως προς τα βήματα που μπορεί να ακολουθήσει κάποιος για να αποκτήσει τα απαιτούμενα προσόντα άσκησης της επαγγέλματος.

| Τεχνικός ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist) | |
|---|---|
| 1η Διαδρομή | Δίπλωμα Ινστιτούτου Επαγγελματικής Κατάρτισης (ΙΕΚ) επιπέδου 5 του ΕΠΠ στις ειδικότητες του Τομέα Πληροφορικής – Συνεχιζόμενη επαγγελματική κατάρτιση για το σύνολο των γνώσεων που αντιστοιχούν στις 2 Κύριες Επαγγελματικές Λειτουργίες του επαγγέλματος (ΚΕΛ 1, ΚΕΛ 2) |
| 2η Διαδρομή | Δίπλωμα Μεταλυκειακού Έτους-Τάξης Μαθητείας επιπέδου 5 του ΕΠΠ στις ειδικότητες του τομέα Πληροφορικής (Τεχνικός Εφαρμογών Πληροφορικής ή Τεχνικός Η/Υ και Δικτύων Η/Υ) – Συνεχιζόμενη επαγγελματική κατάρτιση για το σύνολο των γνώσεων που αντιστοιχούν στις 2 Κύριες Επαγγελματικές Λειτουργίες του επαγγέλματος (ΚΕΛ 1, ΚΕΛ 2) |
| 3η Διαδρομή | Πτυχίο Επαγγελματικού Λυκείου (ΕΠΑ.Λ.) επιπέδου 4 του ΕΠΠ στις ειδικότητες του τομέα Πληροφορικής (Τεχνικός Εφαρμογών Πληροφορικής ή Τεχνικός Η/Υ και Δικτύων Η/Υ) – 1 έτος συναφής επαγγελματική εμπειρία – Συνεχιζόμενη επαγγελματική κατάρτιση για το σύνολο των γνώσεων που αντιστοιχούν στις 2 Κύριες Επαγγελματικές Λειτουργίες του επαγγέλματος (ΚΕΛ 1, ΚΕΛ 2) |
| 4η Διαδρομή | Πτυχίο Επαγγελματικής Σχολής (ΕΠΑ.Σ.) Μαθητείας της ΔΥΠΑ επιπέδου 3 του ΕΠΠ της ειδικότητας «Τεχνίτης Υποστήριξης Συστημάτων Υπολογιστών» – 1,5 έτος συναφής επαγγελματική εμπειρία – Συνεχιζόμενη επαγγελματική κατάρτιση για το σύνολο των γνώσεων που αντιστοιχούν στις 2 Κύριες Επαγγελματικές Λειτουργίες του επαγγέλματος (ΚΕΛ 1, ΚΕΛ 2) |
| 5η Διαδρομή | Απόφοιτοι Δευτεροβάθμιας Εκπαίδευσης (Γενικού Λυκείου) επιπέδου 4 του ΕΠΠ – 2 έτη συναφής επαγγελματική εμπειρία – Συνεχιζόμενη επαγγελματική κατάρτιση για το σύνολο των γνώσεων που αντιστοιχούν στις 2 Κύριες Επαγγελματικές Λειτουργίες του επαγγέλματος (ΚΕΛ 1, ΚΕΛ 2) |

ΕΝΟΤΗΤΑ Ε

# ΕΝΔΕΙΚΤΙΚΟΙ ΤΡΟΠΟΙ ΑΞΙΟΛΟΓΗΣΗΣ ΤΩΝ ΑΠΑΙΤΟΥΜΕΝΩΝ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ



## ΕΝΟΤΗΤΑ Ε «Ενδεικτικοί τρόποι αξιολόγησης των απαιτούμενων γνώσεων και δεξιοτήτων»

Η αξιολόγηση επαγγελματικών γνώσεων και δεξιοτήτων προϋποθέτει την επιλογή της κατάλληλης μεθόδου και των ανάλογων μεθοδολογικών εργαλείων, ανάλογα με το είδος των γνώσεων και δεξιοτήτων που πρόκειται να αξιολογηθούν, τον σκοπό της αξιολόγησης και, ενδεχομένως, τα χαρακτηριστικά του πληθυσμού-στόχου των εργαζόμενων που πρόκειται να αξιολογηθούν ως προς τις γνώσεις και δεξιότητές τους.

Στον πίνακα που ακολουθεί, προτείνονται ενδεικτικοί τρόποι αξιολόγησης του συνόλου των απαιτούμενων Γνώσεων και Δεξιοτήτων ανά Επιμέρους Επαγγελματική Λειτουργία:

| ΕΕΛ | ΠΡΟΤΕΙΝΟΜΕΝΟΣ ΤΡΟΠΟΣ ΑΞΙΟΛΟΓΗΣΗΣ | |
|---|---|---|
| | Γνώσεων | Δεξιοτήτων |
| ΕΕΛ 1.1 | ΤΕΣΤ ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ | ΤΕΣΤ ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ |
| Παρατηρήσεις: | Στο επάγγελμα του «Τεχνικού ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist)» και δεδομένης της γνώσης που ήδη διαθέτουμε για τα μαθησιακά και εκπαιδευτικά χαρακτηριστικά των επαγγελματιών του χώρου, μπορούμε να θεωρήσουμε ότι το σχετικά υψηλό επίπεδο γενικών γνώσεων, αλλά και η εξοικείωση με τη χρήση ηλεκτρονικών υπολογιστών και τεχνολογιών πληροφορικής & επικοινωνιών θα μας έκαναν να προκρίνουμε τη χρήση του τεστ πολλαπλών επιλογών (θεωρητικού και πρακτικού μέρους) ως την προτεινόμενη μέθοδο αξιολόγησης των γνώσεων και των δεξιοτήτων τους.<br><br>Επισημαίνεται ότι από έρευνα που πραγματοποιήσαμε και σε διεθνείς συναφείς πιστοποιήσεις γνώσεων και δεξιοτήτων του επαγγέλματος και εν γένει της Πληροφορικής (CompTIA Security+, (ISC)2 Systems Security Certified Practitioner (SSCP), CompTIA A+, CompTIA Network+ κτλ.), η επικρατούσα μέθοδος αξιολόγησης γίνεται με τεστ πολλαπλών επιλογών. Η δοκιμασία αυτή περιλαμβάνει μια σειρά από ερωτήσεις πολλαπλής επιλογής, οι οποίες έχουν σχεδιαστεί για να αξιολογήσουν πρακτικά τις ικανότητες που συνδέονται με τα καθήκοντα που αντιστοιχούν στο συγκεκριμένο προφίλ και που αφορούν στην ικανότητα αντιμετώπισης συγκεκριμένων καταστάσεων ή προβλημάτων με βάση τη χρήση των ήδη αποκτημένων γνώσεων. | |
| ΕΕΛ 1.2 | ΤΕΣΤ ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ | ΤΕΣΤ ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ |
| Παρατηρήσεις: | Όπως στην ΕΕΛ 1.1 | |
| ΕΕΛ 1.3 | ΤΕΣΤ ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ | ΤΕΣΤ ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ |
| Παρατηρήσεις: | Όπως στην ΕΕΛ 1.1 | |
| ΕΕΛ 2.1 | ΤΕΣΤ ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ | ΤΕΣΤ ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ |
| Παρατηρήσεις: | Όπως στην ΕΕΛ 1.1 | |
| ΕΕΛ 2.2 | ΤΕΣΤ ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ | ΤΕΣΤ ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ |
| Παρατηρήσεις: | Όπως στην ΕΕΛ 1.1 | |

## Περαιτέρω πληροφορίες επαγγέλματος

Το επάγγελμα του «Τεχνικού ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist)» απαιτεί συνεχή εκπαίδευση και ενημέρωση πάνω στο γνωστικό αντικείμενο της Πληροφορικής και ειδικότερα της Ασφάλειας Συστημάτων Πληροφορικής, ώστε οι επαγγελματίες να αντιλαμβάνονται όλες τις εξελίξεις της τεχνολογίας πάνω στο αντικείμενό τους και να εκσυγχρονίζουν την εργασία τους, τις γνώσεις τους και τις δεξιότητές τους.

Έτσι λοιπόν, ο Τεχνικός ασφάλειας συστημάτων πληροφορικής (IT Security Technician/Specialist) μπορεί να ενημερώνεται και να επιμορφώνεται διαρκώς εξ αποστάσεως μέσω on line πλατφορμών εκπαίδευσης. Ενδεικτικά, κάποιοι ιστότοποι που παρέχουν εξ αποστάσεως εκπαίδευση και επιμόρφωση στο γνωστικό αντικείμενο της Πληροφορικής και της Ασφάλειας Πληροφοριών και Κυβερνοασφάλειας με βεβαίωση παρακολούθησης και πιστοποίηση, είναι:

- Εθνική Ακαδημία Ψηφιακών Ικανοτήτων - Gov.gr
- https://nationaldigitalacademy.gov.gr/
- Κέντρο Ανοικτών Διαδικτυακών Μαθημάτων Mathesis
- https://mathesis.cup.gr/
- Udemy: Online Courses / Courses on Demand
- https://www.udemy.com/
- Coursera Degrees, Certificates, & Free Online Courses
- https://www.coursera.org/
- edX Free Online Courses
- https://www.edx.org/

| | |
|---|---|
| ΚΕΛ: | Κύρια Επαγγελματική Λειτουργία |
| ΕΕΛ: | Επιμέρους Επαγγελματική Λειτουργία |
| ΕΕ: | Επαγγελματική Εργασία |
| ΚΕΑ: | Κριτήρια Επαγγελματικής Ανταπόκρισης |
| ΕυΕ: | Εύρος Εφαρμογής |
| Ε.Π. | Επαγγελματικό Περίγραμμα |
| ISCED: | International Standard Classification of Education |
| NQF-ΕΠΠ: | Εθνικό Πλαίσιο Προσόντων |
| ΣΤΕΠ: | Στατιστική ταξινόμηση επαγγελμάτων |
| ΣΤΑΚΟΔ: | Στατιστική ταξινόμηση οικονομικών δραστηριοτήτων |
| ISCO: | Διεθνής Τυποποιημένη Ταξινόμηση Επαγγελμάτων |
| ESCO: | Ευρωπαϊκή ταξινόμηση δεξιοτήτων, ικανοτήτων και επαγγελμάτων |
| ΠΕΠ: | Πλαίσιο εκπαιδευτικών προδιαγραφών προγραμμάτων επαγγελματικής εκπαίδευσης/κατάρτισης |

# Βιβλιογραφία


Καραλής, Θ., Μαρκίδης, Κ., Βαρβιτσιώτη, Ρ., Νάτσης, Π., Καρατράσογλου, Ι., Παπαευσταθίου, Κ., Γούλας, Χ., & Λιντζέρης, Π. (2021) *Μεθοδολογικές προσεγγίσεις ανάπτυξης επαγγελματικών περιγραμμάτων και πλαισίων εκπαιδευτικών προδιαγραφών προγραμμάτων*, Αθήνα: ΙΝΕ ΓΣΕΕ.

William Stallings, (2019), Computer Security: Principles and Practice, Publisher Pearson

Wm. Arthur Conklin, Greg White, Chuck Cothren, Roger Davis, Dwayne Williams, (2018), Principles of Computer Security: CompTIA Security+ and Beyond, 5th Edition, Publisher, McGraw Hill

Νόμος 4624/2019 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων».

Νόμος 4577/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις»

Νόμος 4727/2020 - Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις

Νόμος 4961/2022 «Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις».

Νόμος 5002/2022 «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών»

Νόμος 2121/1993 «Πνευματική Ιδιοκτησία, Συγγενικά Δικαιώματα και Πολιτιστικά Θέματα» (άδειες Creative Commons).

Βίβλος Ψηφιακού Μετασχηματισμού 2020-2025 (https://digitalstrategy.gov.gr/ ).

Εθνική Στρατηγική Κυβερνοασφάλειας (https://mindigital.gr/wp-content/uploads/2020/12/Εθνική-Στρατηγική-Κυβερνοασφάλειας.pdf).

Οδηγός Αυτοαξιολόγησης της Κυβερνοασφάλειας Οργανισμών (Cybersecurity Self Assessment Tool) της Εθνικής Αρχής Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης (https://mindigital.gr/wp-content/uploads/2022/11/Cybersecurity-Self-Assessment-Tool-Greek-version.zip)

Εγχειρίδιο Κυβερνοασφάλειας (Cybersecurity Handbook), της Εθνικής Αρχής Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης

ISO 27001/2022 «Information security, cybersecurity and privacy protection – Information security management systems – Requirements»

ISO/IEC 27005:2022 «Information security, cybersecurity and privacy protection — Guidance on managing information security risks»

ΕΠΑΓΓΕΛΜΑΤΙΚΟ
ΠΕΡΙΓΡΑΜΜΑ

ΠΑΡΑΡΤΗΜΑ

# ΠΛΑΙΣΙΟ ΕΚΠΑΙΔΕΥΤΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ/ΚΑΤΑΡΤΙΣΗΣ

# ΠΑΡΑΡΤΗΜΑ. Πλαίσιο εκπαιδευτικών προδιαγραφών προγραμμάτων επαγγελματικής εκπαίδευσης/κατάρτισης

Σκοπός της ανάπτυξης του Πλαισίου Εκπαιδευτικών Προδιαγραφών Προγραμμάτων Επαγγελματικής Εκπαίδευσης/Κατάρτισης και Γενικής Εκπαίδευσης Ενηλίκων είναι να αποτελέσει έναν εύληπτο, χρηστικό Οδηγό, ο οποίος θα μπορεί να χρησιμοποιηθεί με ευκολία από σχεδιαστές Προγραμμάτων Επαγγελματικής Εκπαίδευσης και Κατάρτισης.

Είναι σαφές ότι το Πλαίσιο Εκπαιδευτικών Προδιαγραφών δεν μπορεί και δεν πρέπει να καλύψει με πληρότητα και ακρίβεια το σύνολο των απαιτήσεων που διαμορφώνουν ένα πρόγραμμα επαγγελματικής εκπαίδευσης και κατάρτισης, για δύο κυρίως λόγους:

α) Τα Επαγγελματικά Περιγράμματα (ΕΠ) σχεδιάζονται με στόχο την κωδικοποίηση της επαγγελματικής και κοινωνικής εμπειρίας ενός συγκεκριμένου εργασιακού αντικειμένου το οποίο διαθέτει ένα ειδικό και αναγνωρίσιμο σώμα γνώσεων, δεξιοτήτων και ικανοτήτων. Είναι λοιπόν δεδομένο ότι η απόκτηση και η ανάπτυξή τους, προϋποθέτει τη διαμόρφωση και τη λειτουργία συγκεκριμένων περιβαλλόντων εκπαίδευσης και κατάρτισης που να ανταποκρίνονται σε συγκεκριμένες μεθοδολογικές και θεσμικές προϋποθέσεις: αναλυτικά προγράμματα επαγγελματικής εκπαίδευσης, προγράμματα αρχικής επαγγελματικής κατάρτισης, συνεχιζόμενης επαγγελματικής κατάρτισης κ.λπ. Τα Πλαίσια Εκπαιδευτικών Προδιαγραφών δεν μπορούν να καλύψουν με ενιαίο και απόλυτο τρόπο το σύνολο των προδιαγραφών όλων των δυνατών εκδοχών εκπαίδευσης και κατάρτισης. Γι' αυτό ακριβώς τον λόγο, περιοριζόμαστε στον προσδιορισμό ενιαίων εκπαιδευτικών προϋποθέσεων και προδιαγραφών, διατυπώνοντας κάποιες ελάχιστες βασικές προδιαγραφές που προηγούνται του κάθε εκπαιδευτικού σχεδιασμού, ανεξάρτητα από τα ιδιαίτερα θεσμικά του χαρακτηριστικά.

β) Τα Πλαίσια Εκπαιδευτικών Προδιαγραφών συντελούν στον εκπαιδευτικό σχεδιασμό προγραμμάτων εκπαίδευσης και κατάρτισης, αλλά σε καμιά περίπτωση δεν μπορούν να υποκαταστήσουν τη διαδικασία σχεδιασμού και διαμόρφωσης ενός συγκεκριμένου προγράμματος εκπαίδευσης και κατάρτισης. Στην πραγματικότητα πρόκειται για δύο εντελώς διαφορετικές διεργασίες οι οποίες υπηρετούν διαφορετικούς στόχους και αξιοποιούν ειδικές και ιδιαίτερες μεθοδολογικές προσεγγίσεις. Ο/η συγγραφέας ενός Επαγγελματικού Περιγράμματος επιδιώκει να αποτυπώσει με ακρίβεια και εγκυρότητα μια συγκεκριμένη επαγγελματική δραστηριότητα, κωδικοποιώντας τα επιμέρους στοιχεία της, έτσι ώστε να εντάσσεται σε έναν ενιαίο και ομοιογενή μηχανισμό συστηματικής κατάταξης επαγγελμάτων. Ο/η σχεδιαστής/ρια ενός εκπαιδευτικού προγράμματος ή ενός προγράμματος κατάρτισης, από την πλευρά του/της, οργανώνει τον χρόνο, τον τόπο και διατάσσει τα αναγκαία διδακτικά μέσα, έτσι ώστε να επιτευχθούν συγκεκριμένα προσδοκώμενα μαθησιακά αποτελέσματα.

Είναι απολύτως κατανοητό ότι στα προκαταρκτικά στάδια ενός εκπαιδευτικού σχεδιασμού επιχειρείται η διερεύνηση των συγκεκριμένων εκπαιδευτικών αναγκών των εκπαιδευομένων και λαμβάνεται υπόψη το συγκεκριμένο θεσμικό πλαίσιο εκπαίδευσης και κατάρτισης. Από αυτή την άποψη, τα ΕΠ είναι μια από τις πολλές δυνατές πηγές τροφοδότησης τόσο σε επίπεδο εκπαιδευτικών περιεχομένων όσο και μεθοδολογικών κατευθύνσεων. Με άλλα λόγια, τα ΕΠ, και πιο συγκεκριμένα τα Πλαίσια Εκπαιδευτικών Προδιαγραφών, προαναγγέλλουν, αλλά δεν καθορίζουν με απόλυτο τρόπο τη μορφή και τη διάρθρωση όλων των δυνατών προγραμμάτων επαγγελματικής εκπαίδευσης και κατάρτισης. Αντίθετα, μπορούν να προτείνουν συγκεκριμένα μεθοδολογικά πλαίσια, τα οποία να συνιστούν ένα είδος ελάχιστης ποιοτικής βάσης ή ακόμη μια δέσμη μεθοδολογικών κατευθύνσεων που να μπορούν να προσανατολίσουν τη διεργασία του εκπαιδευτικού σχεδιασμού προγραμμάτων εκπαίδευσης και κατάρτισης. Στη συνέχεια, αξιοποιώντας το ΕΠ και τις Προδιαγραφές Εκσυγχρονισμένης Μεθοδολογίας, Προτύπων και Εργαλείων Εκπόνησης Επαγγελματικών Περιγραμμάτων και Πλαισίων Προδιαγραφών Προγραμμάτων[11] παρουσιάζεται το Πλαίσιο Εκπαιδευτικών Προδιαγραφών Προγραμμάτων για τον Τεχνικό Ασφάλειας Συστημάτων Πληροφορικής, βάσει των παρακάτω θεμελιωδών ενοτήτων:

1) Ενότητα Προσδοκώμενων μαθησιακών αποτελεσμάτων, όπως περιγράφεται στο ΕΠ με όρους ΕΕΛ και ΚΕΑ.

2) Γενική θεσμική περιγραφή των διαθέσιμων δομών εκπαίδευσης και κατάρτισης.

3) Γενικό προφίλ καταρτιζομένων/εκπαιδευομένων.

4) Γενικό προφίλ εκπαιδευτών.

[11] Καραλής, Θ., Μαρκίδης, Κ., Βαρβιτσιώτη, Ρ., Νάτσης, Π., Καρατράσογλου, Ι., Παπαευσταθίου, Κ., Γούλας, Χ., & Λιντζέρης, Π. (2021) Μεθοδολογικές προσεγγίσεις ανάπτυξης επαγγελματικών περιγραμμάτων και πλαισίων εκπαιδευτικών προδιαγραφών προγραμμάτων, Αθήνα: ΙΝΕ ΓΣΕΕ.

| ΠΛΑΙΣΙΟ ΕΚΠΑΙΔΕΥΤΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ/ΚΑΤΑΡΤΙΣΗΣ ΓΙΑ ΤΟ ΕΠΑΓΓΕΛΜΑ «ΤΕΧΝΙΚΟΣ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ (IT SECURITY TECHNICIAN/SPECIALIST) » | | | |
|---|---|---|---|
| ΕΝΟΤΗΤΕΣ ΠΡΟΣΔΟΚΩΜΕΝΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ | | | |
| Α.<br>«Σχεδιασμός των μέτρων ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού» | Β.<br>«Εφαρμογή και υλοποίηση των μέτρων ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού» | Γ.<br>«Παρακολούθηση και έλεγχος εφαρμογής των μέτρων ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού» | Δ.<br>«Ενημέρωση και υποστήριξη των χρηστών των πληροφοριακών συστημάτων και της Διοίκησης του Οργανισμού σε θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων» |

| | |
|---|---|
| Α.<br>«Σχεδιασμός των μέτρων ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού» | *Τι αναμένεται να κάνει ένας/μία επαγγελματίας, προκειμένου να ανταποκρίνεται με επάρκεια στην **Ενότητα Α** Προσδοκώμενων Αποτελεσμάτων.*<br>• Καταγράφει και απογράφει τα πληροφοριακά συστήματα και τον υπολογιστικό & δικτυακό εξοπλισμό του Οργανισμού που πρέπει να προστατευτούν, τόσο σε επίπεδο υλικού (hardware) και λογισμικού (software) όσο και δικτύων (networks), τηρώντας σχετικό επικαιροποιημένο κατάλογο-μητρώο (inventory).<br>• Εντοπίζει και αναγνωρίζει κινδύνους (ευπάθειες), απειλές και ενέργειες/γεγονότα που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων και προβαίνει στην αξιολόγησή τους, ανάλογα εάν μπορούν να επηρεάσουν/πλήξουν την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και την διαθεσιμότητα (availability) των πληροφοριών και δεδομένων του Οργανισμού, εφαρμόζοντας εργαλεία και μεθοδολογίες. ανάλυσης & διαχείρισης της επικινδυνότητας πληροφοριακών συστημάτων.<br>• Σχεδιάζει και προτείνει τη λήψη των ενδεδειγμένων μέτρων προστασίας και ασφάλειας, με βάση την αξιολόγηση των κινδύνων (risk assessment) που σχετίζονται με τη λειτουργία και χρήση πληροφοριακών συστημάτων και τα διεθνή πρότυπα ασφάλειας πληροφοριών (όπως ISO/IEC 27001, 27002, ISO/IEC 29151, Control Objectives for Information Technology (CobIT), Common Criteria, NIST/SP 800-53, ENISA).<br>• Μελετά προσεκτικά και προσδιορίζει τις ελάχιστες προδιαγραφές ασφάλειας των υπολογιστικών και πληροφοριακών συστημάτων του Οργανισμού, με βάση τα εγχειρίδια και τις οδηγίες χρήσης του κατασκευαστή, καθώς τις οδηγίες της διοίκησης του Οργανισμού ή του Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών, αν υφίσταται.<br>• Συμμετέχει, ενεργά, στο σχεδιασμό, την εκπόνηση και την επικαιροποίηση της Πολιτικής Ασφάλειας. Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων του Οργανισμού, προτείνοντας τη λήψη ενδεδειγμένων μέτρων ασφάλειας, σύμφωνα με τις ανάγκες του Οργανισμού, συνεργαζόμενος προς τούτο με τις οργανικές μονάδες ασφάλειας πληροφοριακών συστημάτων και πληροφορικής του Οργανισμού.<br>• Καταρτίζει και τεκμηριώνει εγγράφως, ακολουθώντας τα διεθνή πρότυπα ασφάλειας πληροφοριών, ειδικότερες πολιτικές, διαδικασίες, τεχνικές και εγχειρίδια ασφάλειας πληροφοριακών συστημάτων, σύμφωνα με τις ανάγκες του Οργανισμού, προκειμένου να προστατευθούν τα στοιχεία του πληροφοριακού συστήματος, αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή.<br>• Αναπτύσσει, σχεδιάζει και επικαιροποιεί, σε περιοδική βάση, λεπτομερές πλάνο αντιμετώπισης και διαχείρισης τυχόν περιστατικών ασφάλειας, καθώς και ανάκτησης δεδομένων και επιχειρησιακής συνέχειας που δύναται να επηρεάσουν τη διαθεσιμότητα, εμπιστευτικότητα ή/και ακεραιότητα των φυσικών ή ηλεκτρονικών πληροφοριακών στοιχείων του Οργανισμού, καταγράφοντας ενέργειες αναγνώρισης, ανίχνευσης και ανάλυσης περιστατικών, περιορισμού και εξάλειψης επιπτώσεων στον Οργανισμό και ανάκτησης δεδομένων. |

| | |
|---|---|
| | *Τι αναμένεται να κάνει ένας/μία επαγγελματίας, προκειμένου να ανταποκρίνεται με επάρκεια στην **Ενότητα Β** Προσδοκώμενων Αποτελεσμάτων.* |
| Β.<br><br>«Εφαρμογή και υλοποίηση των μέτρων ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού» | • Προβαίνει σε ασφαλή διαμόρφωση (secure configuration) εξοπλισμού και εφαρμογών του Οργανισμού, σε σταθμούς εργασίας (desktops, laptops), διακομιστές (servers), δικτυακές συσκευές (routers, switches, ασύρματα access points, firewalls), σε τακτική βάση, περιορίζοντας τη χρήση και εκτέλεση προγραμμάτων και υπηρεσιών στα πληροφοριακά συστήματα, λαμβάνοντας υπόψη τις βέλτιστες πρακτικές και τις οδηγίες ασφάλειας του εκάστοτε προμηθευτή/κατασκευαστή και τα διεθνή πρότυπα ασφάλειας πληροφοριών.<br>• Εφαρμόζει διαδικασίες και μηχανισμούς διαχείρισης, αυθεντικοποίησης και ελέγχου της πρόσβασης των χρηστών, στα πληροφοριακά συστήματα του Οργανισμού, εφαρμόζοντας την αρχή της ελάχιστης λειτουργικότητας (least functionality) και ρυθμίζοντας το σύνολο των συστημάτων, έτσι ώστε να παρέχουν μόνο τις λειτουργίες και υπηρεσίες που υποστηρίζουν την επιχειρησιακή αποστολή του Οργανισμού.<br>• Εφαρμόζει κατάλληλες τεχνολογίες και λαμβάνει τα απαραίτητα μέτρα ασφάλειας για την προστασία της δικτυακής υποδομής του Οργανισμού, εφαρμόζοντας και επικαιροποιώντας κατάλληλους δικτυακούς κανόνες επικοινωνίας, σε περιοδική βάση, χρησιμοποιώντας αποκλειστικά ασφαλή πρωτόκολλα και υπηρεσίες (π.χ. sftp, ssh, https, smbv3).<br>• Λαμβάνει κατάλληλα μέτρα ασφάλειας και προστασίας από κακόβουλο-ιομορφικό λογισμικό και εγκαθιστά, σε τακτικά χρονικά διαστήματα, τις τελευταίες απαραίτητες ενημερώσεις ασφάλειας (Security patches) για τα λειτουργικά συστήματα και τις εφαρμογές του Οργανισμού, σύμφωνα με την υπάρχουσα Πολιτική Ασφάλειας και Προστασίας από Κακόβουλο Λογισμικό.<br>• Αντιμετωπίζει επιθέσεις στα πληροφοριακά συστήματα, δίκτυα και δεδομένα του Οργανισμού εφαρμόζοντας τα προβλεπόμενα πρωτόκολλα και τα κατάλληλα μέτρα.<br>• Υλοποιεί τα απαραίτητα μέτρα και διαδικασίες για την ασφαλή πραγματοποίηση απομακρυσμένης εργασίας από τους εργαζόμενους και την προστασία των κρίσιμων δεδομένων του Οργανισμού, σύμφωνα με την Πολιτική Ασφάλειας Τηλεργασίας και Απομακρυσμένης Πρόσβασης και τις ειδικότερες οδηγίες της διοίκησης του Οργανισμού.<br>• Εφαρμόζει τα ενδεδειγμένα μέτρα κρυπτογράφησης των κρίσιμων δεδομένων και πληροφοριών του Οργανισμού, τόσο κατά την αποθήκευση όσο και κατά τη μετάδοσή τους, ώστε να διασφαλίζεται η εμπιστευτικότητα των δεδομένων και πληροφοριών, και υλοποιεί μηχανισμούς αποτροπής διαρροής τους (π.χ. περιορισμός/απαγόρευση χρήσης φορητών αποθηκευτικών μέσων).<br>• Διασφαλίζει τη διαθεσιμότητα των δεδομένων και πληροφοριών του Οργανισμού, εφαρμόζοντας, περιοδικά, τεχνολογίες και διαδικασίες λήψης αντιγράφων ασφάλειας (backup) και ασφαλούς φύλαξής τους.<br>• Λαμβάνει κατάλληλα μέτρα φυσικής ασφάλειας και περιβαλλοντικής προστασίας του υπολογιστικού και δικτυακού εξοπλισμού του Οργανισμού, καθώς και για την ασφαλή κατάργηση και καταστροφή, τόσο των φυσικών όσο και των ηλεκτρονικών αρχείων και εξοπλισμών, ακολουθώντας τα σχετικά προβλεπόμενα στην Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων του Οργανισμού. |
| | *Τι αναμένεται να κάνει ένας/μία επαγγελματίας, προκειμένου να ανταποκρίνεται με επάρκεια στην **Ενότητα Γ** Προσδοκώμενων Αποτελεσμάτων.* |
| Γ.<br><br>«Παρακολούθηση και έλεγχος εφαρμογής των μέτρων ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού» | • Επιβλέπει, επιθεωρεί και ελέγχει, σε τακτά χρονικά διαστήματα, την εφαρμογή των μέτρων ασφάλειας που έχουν προβλεφθεί και καταγραφεί στην Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων του Οργανισμού, συντάσσοντας σχετική αναφορά (report) προς τη Διοίκηση του Οργανισμού περί των αποτελεσμάτων και ευρημάτων, με προτάσεις για βελτίωση της ασφάλειας, αν απαιτείται.<br>• Συλλέγει συστηματικά (σε πραγματικό χρόνο), συσχετίζει και παρακολουθεί, περιοδικά, με τη βοήθεια κατάλληλων εργαλείων/ πλατφορμών (π.χ. SIEM, Log monitoring tools), τα αρχεία καταγραφής γεγονότων συστήματος και ενεργειών (system, event and application log files) των χρηστών στα κρίσιμα πληροφοριακά συστήματα, για την έγκαιρη ανίχνευση κακόβουλης δραστηριότητας και την αποτελεσματική αντιμετώπιση περιστατικών παραβίασης της ασφάλειας πληροφοριακών συστημάτων, σύμφωνα με την εσωτερικά εφαρμοζόμενη διαδικασία συλλογής τους.<br>• Υλοποιεί, σε περιοδική βάση ή/και κατά την ανάπτυξη/ένταξη συστημάτων και εφαρμογών, τεχνικούς ελέγχους αξιολόγησης των μέτρων ασφάλειας των πληροφοριακών συστημάτων του Οργανισμού (Penetration tests, vulnerability assessment, security code reviews), εφαρμόζοντας εργαλεία ανίχνευσης αδυναμιών ασφάλειας πληροφοριών, κάνοντας χρήση τεχνικών προσομοίωσης κακόβουλων επιθέσεων και προτείνοντας βελτιώσεις όπου απαιτείται. |

| | |
|---|---|
| | • Διενεργεί, σε περιοδική βάση, έλεγχο ακεραιότητας και αξιοπιστίας των αντιγράφων ασφάλειας που λαμβάνονται, καθώς και δοκιμή επαναφοράς δεδομένων (restoration), κατ' ελάχιστο μία (1) φορά ετησίως, σύμφωνα με την εσωτερικά εφαρμοζόμενη πολιτική και διαδικασία λήψης και διαχείρισης αντιγράφων ασφάλειας (Backup).<br>• Ελέγχει επιμελώς τις εφαρμογές και δικτυακές υπηρεσίες πριν την εγκατάσταση ή/και υλοποίησή τους στον Οργανισμό, για τον έγκαιρο εντοπισμό τυχόν ευπαθειών ή κενών ασφάλειας, προτού αυτές μεταβούν σε λειτουργική φάση, λαμβάνοντας υπόψη τις βέλτιστες πρακτικές ή/και τις οδηγίες ασφάλειας του εκάστοτε προμηθευτή/κατασκευαστή.<br>• Ελέγχει και επιθεωρεί, τακτικά, τα μέτρα φυσικής ασφάλειας και περιβαλλοντικής προστασίας του υπολογιστικού και δικτυακού εξοπλισμού του Οργανισμού για τη διαπίστωση της εύρυθμης και ορθής λειτουργίας τους, σύμφωνα με τις ειδικότερες οδηγίες και κατευθύνσεις της διοίκησης του Οργανισμού. |
| Δ.<br>«Ενημέρωση και υποστήριξη των χρηστών των πληροφοριακών συστημάτων και της Διοίκησης του Οργανισμού σε θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων» | *Τι αναμένεται να κάνει ένας/μία επαγγελματίας, προκειμένου να ανταποκρίνεται με επάρκεια στην **Ενότητα Δ** Προσδοκώμενων Αποτελεσμάτων.*<br>• Συμβουλεύει, ενημερώνει και ευαισθητοποιεί, σε τακτά διαστήματα, τους χρήστες υπολογιστικών συστημάτων και τη Διοίκηση του Οργανισμού σε θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων, αξιοποιώντας κάθε πρόσφορο μέσο/τεχνική ενημέρωσης (σεμινάρια, φυλλάδια, γραπτά μηνύματα κτλ.), σε συνεργασία με τον Υπεύθυνο Ασφάλειας Πληροφοριών (CISO) και τον Υπεύθυνο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (DPO) του Οργανισμού, εφόσον υπάρχουν.<br>• Προετοιμάζει το προσωπικό του Οργανισμού για τις απαραίτητες ενέργειες και τρόπους αντίδρασης σε ενδεχόμενο περιστατικό ασφάλειας και παραβίασης προσωπικών δεδομένων, σύμφωνα με το πλάνο αντιμετώπισης και διαχείρισης περιστατικών ασφάλειας, καθώς και ανάκτησης δεδομένων, λειτουργικότητας και επιχειρησιακής συνέχειας, διενεργώντας κατάλληλα προσαρμοσμένες πρακτικές ασκήσεις προσομοίωσης συμβάντων και περιστατικών ασφάλειας.<br>• Τηρεί σχετικό αρχείο-κατάλογο επικαιροποιημένων νομοθετικών κειμένων, κανονισμών κτλ. που σχετίζονται με την ασφάλεια πληροφοριακών συστημάτων, την προστασία προσωπικών δεδομένων και την προστασία δικαιωμάτων χρήσης λογισμικού, παρακολουθώντας συστηματικά τις σχετικές νομοθετικές εξελίξεις.<br>• Καθοδηγεί και υποστηρίζει τεχνικά τους χρήστες των πληροφοριακών συστημάτων και τη διοίκηση του Οργανισμού σε θέματα ασφάλειας που ανακύπτουν, με βάση τη σχετική νομοθεσία και την Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων του Οργανισμού.<br>• Παραλαμβάνει, τηλεφωνικά ή μέσω διαδικτύου, και καταγράφει τις αναφορές των χρηστών για ανακύπτοντα θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων, ιεραρχώντας αυτές ανάλογα με τη σπουδαιότητά τους.<br>• Εντοπίζει, διερευνά με επιμέλεια και επιλύει θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων και δυσλειτουργίες των πληροφοριακών συστημάτων, είτε ύστερα από αναφορές που λαμβάνει είτε όταν αυτά ανακύπτουν από την εφαρμογή και υλοποίηση των μέτρων ασφάλειας<br>• Καταγράφει αναλυτικά και τεκμηριώνει εγγράφως τις λειτουργίες υποστήριξης που εκτελεί, σύμφωνα με τους κανόνες και τις διαδικασίες διαχείρισης και υποστήριξης και τις ειδικότερες οδηγίες του Οργανισμού. |

| ΓΕΝΙΚΗ ΘΕΣΜΙΚΗ ΠΕΡΙΓΡΑΦΗ ΤΩΝ ΔΙΑΘΕΣΙΜΩΝ ΔΟΜΩΝ ΕΚΠΑΙΔΕΥΣΗΣ ΚΑΙ ΚΑΤΑΡΤΙΣΗΣ[12] | |
|---|---|
| Δομές επαγγελματικής εκπαίδευσης: | - |
| Δομές αρχικής επαγγελματικής κατάρτισης: | - |

[12] Αφορά σε δυνατότητες εισόδου σε εκπαιδευτικές δομές είτε διαθέσιμες κατά το παρελθόν ή υφιστάμενες κατά την παρούσα περίοδο ή εν δυνάμει διαθέσιμες σε μελλοντική περίοδο

| | |
|---|---|
| Δομές Συνεχιζόμενης επαγγελματικής κατάρτισης: | - |
| **ΓΕΝΙΚΟ ΠΡΟΦΙΛ ΚΑΤΑΡΤΙΖΟΜΕΝΩΝ /ΕΚΠΑΙΔΕΥΟΜΕΝΩΝ ΑΝΑ ΔΙΑΘΕΣΙΜΗ ΔΟΜΗ ΕΚΠΑΙΔΕΥΣΗΣ ΚΑΙ ΚΑΤΑΡΤΙΣΗΣ[13]** | |
| Δομές επαγγελματικής εκπαίδευσης: | - |
| Δομές αρχικής επαγγελματικής κατάρτισης: | - |
| Δομές Συνεχιζόμενης επαγγελματικής κατάρτισης: | - |

| **ΠΡΟΦΙΛ ΕΚΠΑΙΔΕΥΤΩΝ ΑΝΑ ΕΝΟΤΗΤΑ ΠΡΟΣΔΟΚΩΜΕΝΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ** | | | |
|---|---|---|---|
| **ΕΝΟΤΗΤΕΣ ΠΡΟΣΔΟΚΩΜΕΝΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ** | **ΚΩΔΙΚΟΙ ΣΤΕΠ ΕΚΠΑΙΔΕΥΤΩΝ & ΑΝΑΛΥΤΙΚΗ ΟΝΟΜΑΣΙΑ** | **ΚΩΔΙΚΟΙ ΠΕ/ΤΕ/ΔΕ & ΑΝΑΛΥΤΙΚΗ ΟΝΟΜΑΣΙΑ** (Αν υπάρχει εφαρμογή) | **ΠΑΡΑΤΗΡΗΣΕΙΣ** |
| **Α.** Σχεδίαση των μέτρων ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού. | **2131**: Σχεδιαστές, αναλυτές και Προγραμματιστές συστημάτων υπολογιστών<br>**2139**: Πρόσωπα που αναπτύσσουν επαγγελματική δραστηριότητα στον τομέα της πληροφορικής | **ΠΕ86:** ΠΛΗΡΟΦΟΡΙΚΗΣ (πρώην ΠΕ19 ΠΛΗΡΟΦΟΡΙΚΗΣ Α.Ε.Ι. & ΠΕ20 ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΕΙ) | - |
| **Β.**Εφαρμογή και υλοποίηση των μέτρων ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού | **2131**: Σχεδιαστές, αναλυτές και Προγραμματιστές συστημάτων υπολογιστών<br>**2139**: Πρόσωπα που αναπτύσσουν επαγγελματική δραστηριότητα στον τομέα της πληροφορικής | **ΠΕ86:** ΠΛΗΡΟΦΟΡΙΚΗΣ (πρώην ΠΕ19 ΠΛΗΡΟΦΟΡΙΚΗΣ Α.Ε.Ι. & ΠΕ20 ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΕΙ) | - |

[13] Αφορά την εκπαιδευτική διαδρομή (προφίλ) των απασχολούμενων στην ειδικότητα στην σημερινή αγορά εργασίας

| | | | |
|---|---|---|---|
| | | | |
| **Γ.** Έλεγχος εφαρμογής των μέτρων ασφάλειας πληροφοριακών συστημάτων, δικτύων και πληροφοριών του Οργανισμού | **2131**: Σχεδιαστές, αναλυτές και Προγραμματιστές συστημάτων υπολογιστών<br>**2139**: Πρόσωπα που αναπτύσσουν επαγγελματική δραστηριότητα στον τομέα της πληροφορικής | **ΠΕ86:** ΠΛΗΡΟΦΟΡΙΚΗΣ (πρώην ΠΕ19 ΠΛΗΡΟΦΟΡΙΚΗΣ Α.Ε.Ι. & ΠΕ20 ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΕΙ) | - |
| **Δ.** Ενημέρωση και υποστήριξη των χρηστών των πληροφοριακών συστημάτων σε θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων | **2131**: Σχεδιαστές, αναλυτές και Προγραμματιστές συστημάτων υπολογιστών<br>**2139**: Πρόσωπα που αναπτύσσουν επαγγελματική δραστηριότητα στον τομέα της πληροφορικής | **ΠΕ86:** ΠΛΗΡΟΦΟΡΙΚΗΣ (πρώην ΠΕ19 ΠΛΗΡΟΦΟΡΙΚΗΣ Α.Ε.Ι. & ΠΕ20 ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΕΙ) | - |

ΕΠΑΓΓΕΛΜΑΤΙΚΟ
ΠΕΡΙΓΡΑΜΜΑ

www.ergonesti.gr

ΕΟΠΠΕΠ
ΕΘΝΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΠΡΟΣΟΝΤΩΝ
& ΕΠΑΓΓΕΛΜΑΤΙΚΟΥ ΠΡΟΣΑΝΑΤΟΛΙΣΜΟΥ

Λεωφόρος Εθνικής Αντιστάσεως 41, 14234 Νέα Ιωνία
210 27 09 000 | www.eoppep.gr