ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΡΟΛΟΓΟΣ XXI

ΕΥΧΑΡΙΣΤΙΕΣ XXV

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ XIX

1. ΕΙΣΑΓΩΓΗ 1
1.1. Διαδίκτυο και ηλεκτρονικές πληροφορίες στον 21ο αιώνα ... 1
1.2. Ιστορία του διαδικτύου και της ηλεκτρονικής πληροφορίας – οι πρωτοπόροι του διαδικτύου 12
1.3. Η έννοια της ασφάλειας 19
1.3.1. Ασφάλεια - ανασφάλεια στο διαδίκτυο και φόβος του εγκλήματος 22
1.3.2. Η τεχνική διάσταση του όρου ασφάλεια στα συστήματα ηλεκτρονικών πληροφοριών και στο διαδίκτυο 26
1.3.3. Η έννοια της ασφάλειας στον ελληνικό ΠΚ 27
1.4. Αντικείμενο του παρόντος πονήματος 29

2. ΧΩΡΙΣ ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗ ΣΕ ΗΛΕΚΤΡΟΝΙΚΑ ΔΕΔΟΜΕΝΑ (UNAUTHORIZED ACCESS TO ELECTRONIC DATA) ΚΑΙ HACKING 33
2.1. Ορισμός της έννοιας "hacking" 33
2.2. Ιστορία του hacking 38
2.3. Κατηγοριοποιήσεις των "hackers" 45
2.3.1. Hackers και crackers 45
2.3.2. Διαχωρισμός των hackers ανάλογα με τον σκοπό και το αποτέλεσμα της δράσης τους 47
2.3.3. Διαστρωμάτωση («τάξεις») των hackers 49

2.3.4. Διάκριση των hackers με κριτήριο τη δημιουργική τους ικανότητα 55
2.4. Η εξέλιξη των hackers και τα χαρακτηριστικά τους από την εμφάνιση των ηλεκτρονικών πληροφοριών μέχρι σήμερα 56
2.5. Τα κίνητρα των hackers 60
2.6. Η ηθική των hackers 69
2.7. Η ιδεολογία των hackers 74
2.8. Η (υπο)κουλτούρα του hacking 78
2.9. Ειδικές εκφάνσεις του hacking 82
2.9.1. Ηθικό hacking ("Ethical hacking") 82
2.9.2. "Hacktivism" («ΧΑΚτιβισμός» - παραβιαστές με ακτιβιστική δράση) 84
2.10. Ο «σκοτεινός αριθμός» των περιστατικών hacking (αφανής εγκληματικότητα) 86
2.11. Μέθοδοι και τεχνικές (modi operandi) των hackers για την απόκτηση χωρίς δικαίωμα πρόσβασης 88
2.11.1. Η ανακάλυψη της ταυτότητας του χρήστη – η «κλοπή ταυτότητας» (identity theft) 90
2.11.2. Η πρόσβαση στο σύστημα 92
2.11.2.1. Εξωπρογραμματιστικές πρακτικές hacking 93
2.11.2.1.1. Συλλογή πληροφοριών για το σύστημα (information gathering) 93
2.11.2.1.1.1. «Κοινωνική μηχανική» ("Social engineering") 95
2.11.2.1.1.2. «Κατάδυση στα σκουπίδια» ("Dumpster diving" 96
2.11.2.1.1.3. «Ιχνηλάτηση» ("Footprinting") 97
2.11.2.1.1.4. Shoulder surfing («κρυφοκοίταγμα») 98

2.11.2.1.2. Phishing 99
2.11.2.2. Γνήσιες πρακτικές hacking (χρήση ηλεκτρονικών προγραμμάτων και εντολών) . 102
2.11.2.2.1. Pharming 104
2.11.2.2.2. Επιθέσεις άρνησης υπηρεσίας (DoS και DDoS attacks) ... 106
2.11.2.2.3. Joomla bugs 107
2.11.2.2.4. Packet sniffers 108
2.11.2.2.5. Οι «δούρειοι ίπποι» ("Trojan horses") 108
2.11.2.2.6. «Ιοί» (viruses) και «σκουλήκια» (worms) 109
2.11.2.2.7. IP Spoofing 110
2.11.2.2.8. SQL (Structured Query Language) injection 111
2.11.2.2.9. Hacking shells 112
2.11.2.2.10. Exploits 113
2.11.2.2.11. «Καταγραφή πλήκτρων» ("Key logger") 113
2.11.2.2.12. «Λογικές βόμβες» ("Logic bombs") 114
2.11.2.2.13. Snoopers 114
2.11.2.2.14. «Ανίχνευση ευπαθειών» ("Vulnerability scanning") .. 115
2.11.2.2.15. Source rooting 116
2.11.2.2.16. Bouncing 116
2.11.2.2.17. Rootkits 117
2.11.2.2.18. Υπερχείλιση προσωρινής μνήμης (buffer overflow) 117
2.11.3. Ο hacker μέσα στο σύστημα πληροφοριών 118

3. ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΕΣ ΘΕΩΡΙΕΣ ΓΙΑ ΤΗ ΧΩΡΙΣ ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗ ΣΕ ΗΛΕΚΤΡΟΝΙΚΑ ΔΕΔΟΜΕΝΑ 123
3.1. Θεωρία ορθολογικής επιλογής και παράγωγες θεωρίες 125
3.1.1. Θεωρία ορθολογικής επιλογής 125
3.1.2. Θεωρία της καθημερινής δραστηριότητας ("routine activity theory") 127

3.1.3. Ορθολογική επιλογή προοπτικής (“rational choice perspective”) 129
3.2. Κριτική εγκληματολογία 130
3.3. Θεωρία τεχνικών ηθικής ουδετεροποίησης 132
3.4. Εγκλήματα «λευκού περιλαιμίου» 137
3.5. Η θεωρία της «ηθικής ανάπτυξης» (“moral development theory”) 139
3.6. Η θεωρία της έντασης (“strain theory” / “blocked opportunity theory” - Robert Merton) 140
3.7. Η θεωρία έλλειψης αυτοελέγχου (“self-control theory”- Michael Gottfredson and Travis Hirschi) 142
3.8. “Situational action theory” – “Moral Beliefs and Moral Judgment Theory” 143
3.9. Θεωρία του «διαφορικού συγχρωτισμού» ή της «διαφοροποιούσας συναναστροφής (“differential association theory” – Edwin Sutherland) 145
3.10. Διαχειριστική εγκληματολογία 147

4. ΧΩΡΙΣ ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗ ΣΕ ΗΛΕΚΤΡΟΝΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΟ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ 149
4.1. Τιμώρηση είτε κατά την ωφελιμιστική είτε κατά την ανταποδοτική θεώρηση 150
4.2. Οι hackers και ο ποινικός νόμος 154
4.3. Ειδικές προβληματικές του ποινικού δικαίου σχετικά με το hacking 156
4.3.1. Τόπος τέλεσης του hacking και αρχή ne bis in idem .. 156
4.3.2. Ποινική ευθύνη ή μη του παρόχου πρόσβασης 159
4.4. Επισκόπηση εννόμων τάξεων αναφορικά με το hacking 161
4.4.1. Ελλάδα 162
4.4.1.1. Ο νόμος 1805/1988 162
4.4.1.2. Το άρθρο 4 του νόμου 2246/1994 164
4.4.1.3. Ο νόμος 3674/2008 και η εισαγωγή του άρθρου 292Α ΠΚ 164
4.4.1.4. Ο νόμος 3917/2011 167
4.4.1.5. Ο νόμος 3471/2006 168
4.4.2. Ηνωμένο Βασίλειο 169
4.4.3. Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ) 170
4.4.4. Γερμανία 172

5. ΤΟ ΕΓΚΛΗΜΑ ΤΗΣ ΧΩΡΙΣ ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗΣ ΣΕ ΗΛΕΚΤΡΟΝΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΕΝΝΟΜΗ ΤΑΞΗ 175
5.1. Η διάταξη του άρθρου 370Γ παρ. 2 ΠΚ 175
5.1.1. Εισαγωγικά 175
5.1.2. Προστατευόμενο έννομο αγαθό 177
5.1.3. Έννοια και στοιχεία της αντικειμενικής υπόστασης του εγκλήματος 182
5.1.3.1. Έννοια «στοιχείων» στο ά. 370Γ παρ. 2 185
5.1.3.2. Έννοια απόκτησης πρόσβασης 188
5.1.3.3. Προσέγγιση της έννοιας «χωρίς δικαίωμα» . 195
5.1.3.4. Η έννοια του «νόμιμου κατόχου» 201
5.1.4. Υποκειμενική υπόσταση του εγκλήματος 204
5.1.5. Ποινή του εγκλήματος - Σύγκριση και συρροή με άλλα εγκλήματα 204
5.1.6. Δικονομικά ζητήματα 212
5.2. Το άρθρο 292Α ΠΚ και η σχέση του με το άρθρο 370Γ παρ. 2 ΠΚ 213
5.2.1. Εισαγωγικά 213
5.2.2. Χαρακτηρολογικά στοιχεία των εγκλημάτων του ά. 292Α ΠΚ τα οποία αφορούν σε χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα 214
5.2.3. Περιορισμοί στην εφαρμογή της διάταξης 217
5.2.4. Σχέση ά. 292Α ΠΚ με ά. 370Γ παρ. 2 ΠΚ και ά. 370Α ΠΚ – Το ζήτημα της συρροής 217
5.3. Ο νόμος 3917/2011 και οι ποινικές κυρώσεις του 220
5.3.1. Ο νόμος 3917/2011 και η ενσωμάτωση της Οδηγίας 2006/24/ΕΚ 220
5.3.2. Οι ποινικές κυρώσεις του ά. 11 ν. 3917/2011 223
5.3.3. Συσχέτιση ά. 11 ν. 3917/2011 με ά. 370Γ παρ. 2 και ά. 292Α ΠΚ 225
5.4. Ο νόμος 3471/2006 και οι ποινικές διατάξεις του 227
5.4.1. Ο νόμος 3471/2006 και η ενσωμάτωση της Οδηγίας 2002/58/ΕΚ 227
5.4.2. Οι ποινικές κυρώσεις του ά. 15 ν. 3471/2006 229
5.4.3. Συσχέτιση ά. 15 ν. 3471/2006 με το ά. 11 ν. 3917/2011 και το ά. 370Γ παρ. 2 231

5.5. Νομολογιακή αντιμετώπιση της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα από τα ελληνικά δικαστήρια 232
5.6. Κριτική επισκόπηση και προτάσεις de lege ferenda αναφορικά με την ποινική αντιμετώπιση της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και του hacking 234

6. ΤΟ HACKING ΣΤΑ ΔΙΕΘΝΗ ΚΑΙ ΕΥΡΩΠΑΪΚΑ - ΚΟΙΝΟΤΙΚΑ ΚΕΙΜΕΝΑ 243
6.1. Εισαγωγή 243
6.2. Το hacking και η χωρίς δικαίωμα πρόσβαση σε δεδομένα στο πλαίσιο του Συμβουλίου της Ευρώπης 244
6.2.1. Συστάσεις του Συμβουλίου της Ευρώπης για τα πληροφορικά εγκλήματα 244
6.2.2. Η Σύμβαση του Συμβουλίου της Ευρώπης της 23.11.2001 για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on cyber-crime) 245
6.3. Ευρωπαϊκό ενωσιακό θεσμικό πλαίσιο και ψηφίσματα για το hacking και τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα 253
6.3.1. Η Απόφαση του Συμβουλίου της 31.03.1992 στον Τομέα της Ασφάλειας Συστημάτων Πληροφοριών 254
6.3.2. Η Σύσταση του Συμβουλίου της 07.04.1995 για τα κοινά κριτήρια ασφάλειας της τεχνολογίας πληροφοριών 255
6.3.3. Το Ψήφισμα του Συμβουλίου της 17.02.1997 για το παράνομο και επιβλαβές περιεχόμενο του διαδικτύου 255
6.3.4. Το Ψήφισμα του Συμβουλίου της 28.01.2002 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων 257
6.3.5. Το Ψήφισμα του Συμβουλίου της 18.02.2003 για την ευρωπαϊκή αντίληψη για την ασφάλεια των δικτύων και των πληροφοριών 258

6.3.6. Ο Κανονισμός 460/2004 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών 259
6.3.7. Η Απόφαση Πλαίσιο της 24.02.2005 για τις επιθέσεις κατά των συστημάτων πληροφοριών 261
6.3.8. Η Ανακοίνωση της Επιτροπής της 15.11.2006 σχετικά με την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού 269
6.3.9. Η Ανακοίνωση της Επιτροπής της 22.05.2007 προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο 270
6.3.10. Το Ψήφισμα του Συμβουλίου της 18.12.2009 για μια ευρωπαϊκή συνεργατική προσέγγιση όσον αφορά την ασφάλεια δικτύων και πληροφοριών 271
6.3.11. Η Ανακοίνωση της Επιτροπής της 22.11.2010 για τη «στρατηγική εσωτερικής ασφάλειας της ΕΕ στην πράξη: πέντε βήματα για μια ασφαλέστερη Ευρώπη» 273
6.3.11.1. Το περιεχόμενο της ανακοίνωσης για την πρόληψη του κυβερνοεγκλήματος 273
6.3.11.2. Η δημιουργία του ευρωπαϊκού κέντρου για τα εγκλήματα στον κυβερνοχώρο (EC3) 274
6.3.12. Ο Κανονισμός υπ' αρ. 526/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 21.05.2013 σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και την κατάργηση του κανονισμού (ΕΚ) αρ. 460/2004 275
6.3.13. Η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12.08.2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου 276

7. ΕΡΕΥΝΑ ΣΕ ΝΟΜΙΚΟΥΣ, ΕΠΙΣΤΗΜΟΝΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ (ΔΙΑΧΕΙΡΙΣΤΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΔΕΔΟΜΕΝΩΝ) ΚΑΙ HACKERS 285
7.1. Ο στόχος της έρευνας 285
7.2. Οι υποθέσεις της έρευνας 287
7.2.1. Η σύγχρονη έννοια της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά συστήματα πληροφοριών και δεδομένα και του hacking 287
7.2.2. Ιδεολογία ή οικονομικό όφελος/ οικονομική ζημία; ... 288
7.2.3. Έλεγχος γενικοπροληπτικής αποτελεσματικότητας της ελληνικής ποινικής νομοθεσίας και προτάσεις de lege ferenda για τη σύγχρονη νομοθετική αντιμετώπιση του hacking 290
7.2.4. Εναλλακτικοί τρόποι ενίσχυσης της ασφάλειας των ηλεκτρονικών συστημάτων πληροφοριών και δεδομένων 292
7.3. Η ταυτότητα της έρευνας 293
7.3.1. Μορφές και φύση της έρευνας 294
7.3.1.1. Διερευνητική έρευνα 294
7.3.1.2. Περιγραφική έρευνα 295
7.3.1.3. Επεξηγητική έρευνα 296
7.3.1.4. Έρευνα αξιολόγησης 297
7.3.1.5. Έρευνα σε δείγμα σκοπιμότητας 299
7.3.1.6. Έρευνα με πρωτογενή δεδομένα 304
7.3.2. Μέθοδος και τεχνική της έρευνας 306
7.3.2.1. Συνδυασμός ποιοτικής και ποσοτικής έρευνας 306
7.3.2.2. Τεχνικές της έρευνας (ερωτηματολόγιο και επικουρικά συνέντευξη με hackers και ανάλυση περιεχομένου και δευτερογενών δεδομένων) 309
7.4. Η ερευνητική ομάδα 312
7.5. Ο εντοπισμός του δείγματος της έρευνας 313
7.5.1. Κατάρτιση, κοινοποίηση και συμπλήρωση των ερωτηματολογίων 313
7.5.2. Η προβληματική της χρήσης του διαδικτύου ως εργαλείου στην έρευνα 315

7.5.3. Το δείγμα των νομικών 317
7.5.4. Το δείγμα των επιστημόνων πληροφορικής (προγραμματιστές, τεχνικοί δικτύων ηλεκτρονικών υπολογιστών και διαχειριστές ηλεκτρονικών δεδομένων) 318
7.5.5. Το δείγμα των hackers 319
7.5.5.1. Οι hackers στην Ελλάδα 319
7.5.5.2. Η δυσκολία της ανεύρεσης δείγματος hackers 320
7.5.5.3. Η προσέγγιση ομάδων hackers στην Ελλάδα 322
7.5.5.4. Η Ελληνική Χάκινγκ Σκηνή (Greek Hacking Scene) – Ανάλυση περιεχομένου της επικοινωνίας 323
7.5.5.5. Η ομάδα hackerspace.gr – Ανάλυση περιεχομένου της επικοινωνίας – Ανοιχτή συνέντευξη με δύο μέλη της ομάδας 330
7.6. Περιορισμοί της έρευνας 336
7.7. Τα ερωτηματολόγια 341
7.7.1. Γενικές επισημάνσεις για τη διατύπωση των ερωτήσεων 342
7.7.2. Δημογραφικά στοιχεία 344
7.7.3. Τα ερωτηματολόγια για το δείγμα νομικών και το δείγμα επιστημόνων πληροφορικής 345
7.7.4. Το ερωτηματολόγιο για το δείγμα hackers 354
7.8. Αποτελέσματα της έρευνας 364
7.8.1. Δείγμα νομικών 364
7.8.1.1. Απαντήσεις 364
7.8.1.2. Συνολική θεώρηση απαντήσεων δείγματος νομικών 386
7.8.2. Δείγμα επιστημόνων πληροφορικής (τεχνικών ασφαλείας και υπεύθυνων διαχείρισης ηλεκτρονικών δεδομένων) 389
7.8.2.1. Απαντήσεις 389
7.8.2.2. Συνολική θεώρηση απαντήσεων δείγματος επιστημόνων πληροφορικής 412
7.8.3. Συσχέτιση απαντήσεων νομικών και επιστημόνων πληροφορικής 414

7.8.3.1. Τι είναι hacking σύμφωνα με την εμπειρία σας; 415
7.8.3.2. Πιστεύετε ότι οι hackers ενεργούν περισσότερο με βάση ιδεολογικά κίντρα ή με σκοπό το οικονομικό όφελος; 415
7.8.3.3. Θεωρείτε ότι οι έλληνες νομικοί που ασχολούνται με το δίκαιο της πληροφορικής είναι επαρκώς ενημερωμένοι και εκπαιδευμένοι σε θέματα πληροφορικής και ιδίως hacking; / Θεωρείτε ότι οι έλληνες επιστήμονες πληροφορικής είναι επαρκώς ενημερωμένοι σε σύγχρονα θέματα ασφάλειας των ηλεκτρονικών δεδομένων 416
7.8.3.4. Πιστεύετε ότι οι δράσεις των hackers μπορούν να έχουν θετική συμβολή στην κοινωνία; Αν ναι, σε ποιες περιπτώσεις; 417
7.8.3.5. Κατά τη γνώμη σας, η ελληνική νομοθεσία είναι αποτελεσματική για τη διαφύλαξη της ασφάλειας των ηλεκτρονικών δεδομένων; 418
7.8.3.6. Πρέπει να είναι ελεύθερη η πρόσβαση στην πληροφορία στο διαδίκτυο; Αν ναι, σε ποιες περιπτώσεις; 419
7.8.3.7. Έχετε να προτείνετε άλλα μέτρα – πέρα από ποινικές διατάξεις – που μπορούν να ληφθούν για την προαγωγή της ασφάλειας των ηλεκτρονικών δεδομένων; Αν ναι, ποια; 420
7.8.3.8. Πόσο ασφαλής νιώθετε αναφορικά με τα ηλεκτρονικά σας δεδομένα στο διαδίκτυο; .. 421
7.8.3.9. Ποια η γνώμη σας: χρειάζεται αυστηροποίηση των ποινικών κυρώσεων, αποποινικοποίηση του hacking ή οι νομικές προβλέψεις να μείνουν ως έχουν; 421
7.8.3.10. Όποιος αποκτά χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα στο διαδίκτυο με σκοπό οικονομικό όφελος ή πρόκληση

ζημίας πρέπει να έχει την ίδια, ηπιότερη ή αυστηρότερη ποινική μεταχείριση από τον νόμο σε σχέση με αυτόν που δεν έχει σκοπό το οικονομικό όφελος ή την πρόκληση ζημίας; (ερώτηση 10 του ερωτηματολογίου των νομικών και ερώτηση 12 του ερωτηματολογίου των επιστημόνων πληροφορικής) 422
7.8.4. Δείγμα hackers 423
7.8.4.1. Απαντήσεις 423
7.8.4.2. Συνολική θεώρηση απαντήσεων δείγματος hackers 455

8. ΣΥΣΧΕΤΙΣΗ ΠΟΡΙΣΜΑΤΩΝ ΕΡΕΥΝΑΣ ΣΕ ΣΥΝΑΡΤΗΣΗ ΚΑΙ ΜΕ ΤΙΣ ΥΠΟΘΕΣΕΙΣ ΤΗΣ ΕΡΕΥΝΑΣ 463
8.1. Η σύγχρονη ένοια της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά συστήματα πληροφοριών και δεδομένα και του hacking 463
8.2. Το κίνητρο των hackers 465
8.3. Έλεγχος γενικοπροληπτικής αποτελεσματικότητας της ελληνικής ποινικής νομοθεσίας και προτάσεις de lege ferenda για τη σύγχρονη νομοθετική αντιμετώπιση του hacking 467
8.4. Εναλλακτικοί τρόποι ενίσχυσης της ασφάλειας των ηλεκτρονικών συστημάτων πληροφοριών και δεδομένων 470

9. ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ 475
9.1. Τεχνικές και πρακτικές για την ασφάλεια των ηλεκτρονικών συστημάτων πληροφοριών 476
9.1.1. Έλεγχος της πρόσβασης – προφύλαξη ηλεκτρονικών δεδομένων..... 476
9.1.2. Χρήση τεχνολογικών κατασκευών για την ασφάλεια των πληροφοριών (αυτοματοποιημένα συστήματα ανίχνευσης – βιομετρικός έλεγχος – «πύρινα τείχη»…) 477

9.1.3. Σωστή λειτουργία της επιχείρησης αναφορικά με την ασφάλεια των ηλεκτρονικών πληροφοριών 480
9.1.4. Αξιοποίηση της πείρας και κατάρτισης των hackers .. 481
9.1.5. Κρυπτογραφία 482
9.2. Ηθική διαπαιδαγώγηση, ενημέρωση και εκπαίδευση 485
9.3. Αυτορρύθμιση (self-regulation) 490
9.4. Ανάγκη διεθνοποίησης μέτρων για το κυβερνοέγκλημα 492

10. ΣΥΝΟΨΗ ΣΥΜΠΕΡΑΣΜΑΤΩΝ 499

11. ΕΠΙΜΥΘΙΟ 507

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ Ι: ΑΠΑΝΤΗΣΕΙΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ ΔΕΙΓΜΑΤΟΣ ΝΟΜΙΚΩΝ 515
ΠΑΡΑΡΤΗΜΑ ΙΙ: ΑΠΑΝΤΗΣΕΙΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ ΔΕΙΓΜΑΤΟΣ ΕΠΙΣΤΗΜΟΝΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ 515
ΠΑΡΑΡΤΗΜΑ ΙΙΙ: ΑΠΑΝΤΗΣΕΙΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ ΔΕΙΓΜΑΤΟΣ HACKERS 515
ΠΑΡΑΡΤΗΜΑ IV: ΕΠΙΣΤΟΛΗ ΤΗΣ GREEK HACKING SCENE 517
ΠΑΡΑΡΤΗΜΑ V: ΣΥΝΟΔΕΥΤΙΚΗ ΚΑΙ ΕΝΗΜΕΡΩΤΙΚΗ ΕΠΙΣΤΟΛΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ 529

ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΡΘΡΟΓΡΑΦΙΑ 531

ΔΙΑΔΙΚΤΥΑΚΟΙ ΤΟΠΟΙ 559

ΔΗΜΟΣΙΕΥΜΑΤΑ ΕΦΗΜΕΡΙΔΩΝ ΚΑΙ ΕΝΗΜΕΡΩΤΙΚΩΝ ΙΣΤΟΣΕΛΙΔΩΝ – ΔΕΛΤΙΑ ΤΥΠΟΥ (ΕΝΔΕΙΚΤΙΚΑ) 579