ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Malaga, R., A. (2005). *Εισαγωγή στην Τεχνολογία Πληροφοριακών Συστημάτων*: Μ. Γκιούρδας.
[2] Κάτσικας, Σ., Κ. (2014). *Διαχείριση Της Ασφάλειας Πληροφοριών*: ΠΕΔΙΟ.
[3] Κάτσικας, Σ. & Γκρίτζαλης, Δ. & Γκρίτζαλης. (2004). *Ασφάλεια Πληροφοριακών Συστημάτων*: ΝΕΩΝ ΤΕΧΝΟΛΟΓΙΩΝ.
[4] Strebe, M. (2004). *Ασφάλεια Δικτύων – Εισαγωγή στη Σύγχρονη Τεχνολογία*: Μ. Γκιούρδας.
[5] Πάγκαλος, Γ. & Μαυρίδης, Ι. (2002). *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων:* ΑΝΙΚΟΥΛΑ.
[6] Scambray, J. & Kurtz, G. & Mcclure, S. (2001). *ΧΑΚΕΡ ΕΠΙΘΕΣΗ ΚΑΙ ΑΜΥΝΑ*: Μ. Γκιούρδας.
[7] Ηλεκτρονικό Έγκλημα. www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414
[8] Tanenbaum A. S. (2009). *ΣΥΓΧΡΟΝΑ ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ*: ΚΛΕΙΔΑΡΙΘΜΟΣ.
[9] Tanenbaum A. S. (2003). *Δίκτυα Υπολογιστών*: ΚΛΕΙΔΑΡΙΘΜΟΣ.
[10] Chaffey, D. (2002). *Ηλεκτρονικό Επιχειρείν και Ηλεκτρονικό Εμπόριο*: ΚΛΕΙΔΑΡΙΘΜΟΣ.
[11] Schneider G. P. (2015). *ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ*: Μ. Γκιούρδας.
[12] Πασχόπουλος Α., Σκαλτσάς Π. (2006). *Ηλεκτρονικό Εμπόριο: Επιχειρηματική στρατηγική και marketing στο Διαδίκτυο*: ΚΛΕΙΔΑΡΙΘΜΟΣ.
[13] Τα άρθρα που ορίζουν την Αρχή Προστασίας Προσωπικών Δεδομένων (Ν. 2472/1997: 15-20) *http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#1*
[14] Mitnik, K. D. (2002). *The Art of Deception*: John Wiley & Sons.
[15] What Motivates Cyber-Attackers?, 10/2014, Chen Han, Rituja Dongre http://timreview.ca/article/838
[16] Understanding Denial-Of-Service Attacks. https://www.us-cert.gov/ncas/tips/ST04-015
[17] Paxson V. An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks. http://www.icir.org/vern/papers/reflectors.CCR.01.pdf
[18] Ramzan, Z. (2010). *Handbook of Information and Communication Security*: Springer.\
[19] Gyongyi Z. & Garcia-Molina H. Web Spam Taxonomy. http://airweb.cse.lehigh.edu/2005/gyongyi.pdf
[20] PayPal Purchase Protection, πηγή: https://www.paypal.com/us/webapps/mpp/paypal-safety-and-security
[21] Ερωτήσεις και απαντήσεις σχετικά με το Bitcoin: https://bitcoin.org/el/faq
[22] PayPal Obtains Bank Charter for European Union,15/05/2007, Paymentsnews.com , http://www.paymentsnews.com/2007/05/paypal_obtains_.html
[23] Η εργασία του «άγνωστου» δημιουργού του BitCoin. Πηγή: https://bitcoin.org/bitcoin.pdf
[24] Menezes, A., Oorschot, P., Vanstone, S. (1996). *Handbook of Applied Cryptography*: CRC Press.
[25] Dictionary Attacks 101, 01/2009, McConnell, Steven C. https://blog.codinghorror.com/dictionary-attacks-101/
[26] Margaret R. J., *Internet Commerce The Emerging Legal Framework* 1174–1175, 2006, Foundation Press.
[27] Οδηγία31/2000/ΕΚ: http://eurlex.europa.eu/legalcontent/EL/TXT/PDF/?uri=CELEX:32000L0031&from=EL
[28] Οδηγία 2011/83/ΕΕ: http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32011L0083&from=EL
[29] Κανονισμός 910/2014/ΕΕ: http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32014R0910&from=EL
[30] Π.Δ. 131/2003 : http://dide.flo.sch.gr/Plinet/Nomothesia-Internet/PD.131-2003.pdf
[31] Η Ιστορία του PayPal http://www.fundinguniverse.com/company-histories/paypal-inc-history/
[32] Σελίδα της Ευρωπαϊκής Commission σχετικά με τον 2016/679 - http://ec.europa.eu/justice/data-protection/reform/index_en.htm

ΠΑΡΑΡΤΗΜΑΤΑ

ΝΟΜΟΘΕΣΙΑ

Ελληνική νομοθεσία σχετικά με το Διαδικτυακό Έγκλημα

Ο Ν. 1805/88, αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes) και στο βαθμό που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον Διαδικτύου (Internet), τότε τα άρθρα αυτά εφαρμόζονται και στις συγκεκριμένες περιπτώσεις. Στην ελληνική νομοθεσία όμως, δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του Διαδικτύου από άποψη Ποινικού Δικαίου. Ως εκ τούτου, η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων διεθνών οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων. Ανεξάρτητα όμως από το εάν ο ανωτέρω νόμος και οι διεθνείς συνεργασίες επαρκούν ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της Πληροφορικής, το βέβαιον είναι ότι, δεν επαρκούν για την τελεία αντιμετώπιση των εγκλημάτων που έχουν τελεστεί με τη χρήση του Διαδικτύου. Πρόσφατα τέθηκε σε ισχύ το Π.Δ. 47/2005, από την Α.Δ.Α.Ε. (Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών), το οποίο αφορά τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του. Ενώ, σύντομα αναμένεται να τεθεί σε ισχύ η Συνθήκη της Βουδαπέστης.

Άρθρο 370Β

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών. Ως απόρρητα θεωρούνται κι εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.
2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.
3. Αν πρόκειται για στρατιωτικό ή διαπλαστικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παρ. 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.
4. Οι πράξεις που προβλέπονται στις παρ.1 και 2 διώκονται ύστερα από έγκληση.
άρθρο 370Γ
1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.
2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.
4. Οι πράξεις των παρ. 1 έως 3 διώκονται ύστερα από έγκληση.

Άρθρο 386Α - Απάτη με υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα.