ΣΧΕΔΙΟ ΜΑΘΗΜΑΤΟΣ

ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ*	**ΚΖ'**
ΤΜΗΜΑ*	**ΟΛΑ**
ΚΥΚΛΟΣ*	**ΚΖ_Α' ΚΥΚΛΟΣ ΕΙΔΙΚΗΣ ΦΑΣΗΣ ΣΠΟΥΔΩΝ**
Τίτλος*	Κυβερνοασφάλεια στη Δημόσια Διοίκηση
Συνολικές Ώρες*	23 (21+2 εξέταση)
Σύντομη Περιγραφή	Τα μελλοντικά ανώτερα στελέχη της Δημόσιας Διοίκησης πρέπει να κατανοήσουν ότι το πρόβλημα της ασφάλειας ψηφιακών συστημάτων είναι πολυδιάστατο και πέραν της προστασίας από απειλές (εγκληματικές ενέργειες, δολιοφθορές, κατασκοπεία, ατυχήματα και αστοχίες), στους σχετικούς κινδύνους συμπεριλαμβάνονται και αυτοί που αφορούν στη μείωση της εμπιστοσύνης και αξιοπιστίας των φορέων προς τους πολίτες, οι οποίοι αν δεν αντιμετωπιστούν, είναι δυνατόν να επηρεάσουν αρνητικά τη σταθερότητα της Δημόσιας Διοίκησης. Ολοκληρώνοντας το μάθημα, θα πρέπει να είναι σε θέση να κατανοήσουν με λεπτομέρεια τις βασικές έννοιες της εν λόγω επιστημονικής περιοχής και να εκτιμήσουν τις συνέπειες των κινδύνων που αντιμετωπίζουν στον κυβερνοχώρο, να εφαρμόζουν με επιτυχία μεθόδους και τεχνολογίες προστασίας πληροφοριακών συστημάτων και δικτύων και να γνωρίζουν τις μεθοδολογίες και τις διαδικασίες που απαιτούνται για τη διαχείριση περιστατικών ασφαλείας αλλά και την διασφάλιση της επιχειρησιακής συνέχειας των φορέων της Δημόσιας Διοίκησης.
Στόχος Μαθήματος	Το μάθημα περιλαμβάνει εισαγωγή στην ανάγκη προστασίας των πληροφοριών και την παρουσίαση βασικών εννοιών ασφάλειας των ψηφιακών συστημάτων (προσδιορισμός και επεξήγηση εννοιών, επιθέσεις και απειλές, κακόβουλο λογισμικό, ταυτοποίηση και αυθεντικοποίηση). Στη συνέχεια θα παρουσιαστεί η λογική για τη Διακυβέρνηση Κυβερνοασφάλειας, η εθνική αρχή και άλλοι εμπλεκόμενοι, αλλά και οι αναγκαίες πολιτικές και τα μέτρα ασφάλειας. Τέλος, απαιτείται εξοικείωση των σπουδαστών/τριών με τη διαχείριση, προκειμένου να υπάρχει ο απαραίτητος Έλεγχος

* Τα πεδία συμπληρώνονται από την ΕΣΔΔΑ

	Ασφάλειας Πληροφοριών. Τέλος, έμφαση δίδεται στη διασφάλιση επιχειρησιακής συνέχειας μέσω του σχεδιασμού ανάκαμψης από καταστροφές (βασικές έννοιες, διαδικασίες, τεχνικές).
Ειδικοί στόχοι:	
1. Γνώσεις	• Η κατανόηση των αρχών κυβερνοασφάλειας • Η αναγνώριση των διαφορετικών τύπων επιθέσεων • Η εξοικείωση με τις βασικές έννοιες κυβερνοασφάλειας • Η κατανόηση των διατάξεων για την κυβερνοασφάλεια • Η επεξεργασία πολιτικών και διαδικασιών ασφάλειας πληροφοριακών συστημάτων και δικτύων
2. Δεξιότητες	• Η εφαρμογή των μέτρων ασφάλειας στις επιχειρησιακές διαδικασίες • Η επιλογή των κατάλληλων μέτρων προστασίας για την εφαρμογή ενός σχεδίου ασφάλειας • Η διαμόρφωση πολιτικών και διαδικασιών ασφάλειας • Η σχεδίαση δράσεων για τη βελτίωση του επιπέδου ασφάλειας των φορέων της Δημόσιας Διοίκησης
3. Στάσεις/Συμπεριφορές	• Να είναι θετικοί στην υιοθέτηση πρωτοβουλιών για την θωράκιση των πληροφοριακών συστημάτων και δικτύων των φορέων της Δημόσιας Διοίκησης • Να προάγουν δράσεις ενημέρωσης και επιμόρφωσης του προσωπικού σε θέματα κυβερνοασφάλειας • Να συμβάλλουν στην εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας και των σχετικών οδηγιών

Μέθοδοι Διδασκαλίας / Εκπαιδευτικές Τεχνικές	**Διάλεξη – Συζήτηση – Ομάδες Εργασίας – Καταιγισμός Ιδεών – Μελέτη Περίπτωσης**	
Τρόπος εξέτασης (Σημειώστε με Χ)		Συμμετοχή στο μάθημα και εκπόνηση τριών μελετών περίπτωσης με παρουσίαση
	Χ	Εκπόνηση ατομικής εργασίας με παρουσίαση - Βαρύτητα: 100%
		Άλλη, προσδιορίστε:
Προϋποθέσεις Υποδομών	Εργαστήριο ανάλογου μεγέθους και αριθμού Η/Υ με τον αριθμό των εκπαιδευομένων. Εγκατεστημένο Microsoft Office, Adobe Reader, 7-zip	
Απαραίτητα Εκπαιδευτικά Μέσα	Video projector και Η/Υ με εγκατεστημένο το Microsoft Word, Microsoft Power Point και 7-zip για παρουσίαση εκπαιδευτικών διαφανειών.	
Απαραίτητο Λογισμικό	Microsoft Office & Adobe Reader	
Είδος Εκπαιδευτικού Υλικού που παραδίδεται (Σημειώστε με Χ)	Χ	Σημειώσεις Εισηγητή
	Χ	Παρουσιάσεις Εισηγητή
		Μελέτες Περίπτωσης
		Άρθρα – Μελέτες – Αποσπάσματα

	X	Κανονιστικό Πλαίσιο
		Πρότυπα
		Εγχειρίδια Χρήσης
		Ψηφιακό Υλικό – Λογισμικό
	X	Διαδικτυακοί Τόποι
	X	Σχετική Βιβλιογραφία

ΑΝΑΛΥΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΑΝΑ ΔΙΔΑΚΤΙΚΗ ΕΝΟΤΗΤΑ[1]	
α/α Διδακτικής Ενότητας	**1**
Τίτλος Διδακτικής Ενότητας	**Βασικές Έννοιες Κυβερνοασφάλειας**
Αναλυτική Περιγραφή Διδακτικής Ενότητας	• Εισαγωγή στην κυβερνοασφάλεια • Αρχές κυβερνοασφάλειας • Απαιτήσεις ασφάλειας • Ορισμοί • Είδη επιθέσεων • Ιομορφικό λογισμικό Παραδείγματα
Διάρκεια (ώρες)	**3**
Εκπαιδευτικές τεχνικές (ενδεικτικά: εργαστήριο, μελέτη περίπτωσης, εργασία, άσκηση κ.ά.)	**Διάλεξη – Συζήτηση – Καταιγισμός Ιδεών – Ομάδες Εργασίας**
Βασικό Εκπαιδευτικό Υλικό (όπως παρουσιάσεις διδασκόντων, ενότητες βιβλίων, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• CYDERSECURITY_ESDD_2021_enotita_1.pdf • Εκπαιδευτικό υλικό ΕΣΔΔΑ, CYBERSECURITY.pdf
Ενδεικτικό Εκπαιδευτικό Υλικό (όπως βιβλία, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών: http://www.adae.gr/ • Ερωτηματολόγιο της ΑΔΑΕ: http://www.adae.gr/quiz/ • Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: http://www.dpa.gr/ • Ερωτηματολόγιο υποκλοπή ταυτότητας: https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/SELF_ASSESSMENT_TEST/INDEX.HTML • Network Security Essentials: Applications and Standards (6th Edition), by William Stallings, Pearson Education Limited, 2017. • Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, επιστημονική επιμέλεια Κωνσταντίνος Λαμπρινουδάκης, Λίλιαν Μήτρου, Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας. Εκδόσεις Παπασωτηρίου 2010. • Ασφάλεια Πληροφοριακών Συστημάτων, επιστημονική επιμέλεια, Σωκράτης Κάτσικας, Δημήτρης Γκρίτζαλης, Στέφανος Γκρίτζαλης, Εκδόσεις Νέων Τεχνολογιών, 2004.
α/α Διδακτικής Ενότητας	**2**
Τίτλος Διδακτικής Ενότητας	**Εθνικές Στρατηγικές Κυβερνοασφάλειας**
Αναλυτική Περιγραφή Διδακτικής Ενότητας	• Ευρωπαϊκή Στρατηγική Κυβερνοασφάλειας • Χάραξη Στρατηγικής Κυβερνοασφάλειας • Εθνική Στρατηγική Κυβερνοασφάλειας • Κριτήρια Αξιολόγησης Παράδειγμα – μελέτη περίπτωσης

[1] Συμπληρώνεται για κάθε διδακτική ενότητα ξεχωριστά.

Διάρκεια (ώρες)	**3**
Εκπαιδευτικές τεχνικές (ενδεικτικά: εργαστήριο, μελέτη περίπτωσης, εργασία, άσκηση κ.ά.)	**Διάλεξη – Συζήτηση – Καταιγισμός Ιδεών – Ομάδες Εργασίας – Πρακτική Εξάσκηση**
Βασικό Εκπαιδευτικό Υλικό (όπως παρουσιάσεις διδασκόντων, ενότητες βιβλίων, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• CYBERSECURITY_ESDD_2021_enotita_2.pdf • Εκπαιδευτικό υλικό ΕΣΔΔΑ, CYBERSECURITY.pdf
Ενδεικτικό Εκπαιδευτικό Υλικό (όπως βιβλία, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• BSA | The Software Alliance (2015). *EU Cybersecurity Dashboard/ A Path to a Secure European Cyberspace*. EU Cybersecurity Maturity Dashboard. • ENISA (2016). *NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies*. European Network and Information Security Agency. DOI: 10.2824/48036. • ENISA (2014). *An evaluation Framework for National Cyber Security Strategies*. European Network and Information Security Agency. DOI: 10.2824/3903. • ENISA (2012a). *National Cyber Security Strategies – Practical Guide on Development and Execution*. European Network and Information Security Agency. • ENISA (2012b). *National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace*. European Network and Information Security Agency. • European Commission (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. JOIN(2013) 1 final, Brussels. • Εθνική Στρατηγική Κυβερνοασφάλειας (2018). Υπουργική Απόφαση αριθμ. πρωτ. 3218/07-03-2018 (ΑΔΑ: Ψ4Ρ7465ΧΘ0-Ζ6Ω).
α/α Διδακτικής Ενότητας	**3**
Τίτλος Διδακτικής Ενότητας	**Πολιτικές Ασφάλειας**
Αναλυτική Περιγραφή Διδακτικής Ενότητας	• Ανάγκη Θέσπισης Πολιτικής Ασφάλειας • Οφέλη Πολιτικών Ασφάλειας • Ανάπτυξη Πολιτικής Ασφάλειας • Κατηγορίες Μέτρων Ασφάλειας • Κρίσιμοι Παράγοντες Επιτυχίας Παράδειγμα – μελέτη περίπτωσης
Διάρκεια (ώρες)	**3**
Εκπαιδευτικές τεχνικές (ενδεικτικά: εργαστήριο, μελέτη περίπτωσης, εργασία, άσκηση κ.ά.)	**Διάλεξη – Συζήτηση – Καταιγισμός Ιδεών – Ομάδες Εργασίας**
Βασικό Εκπαιδευτικό Υλικό	• CYBERSECURITY_ESDD_2021_enotita_3.pdf

(όπως παρουσιάσεις διδασκόντων, ενότητες βιβλίων, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• Εκπαιδευτικό υλικό ΕΣΔΔΑ, SECURITY.pdf
Ενδεικτικό Εκπαιδευτικό Υλικό (όπως βιβλία, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• Network Security Essentials: Applications and Standards (6th Edition), by William Stallings, Pearson Education Limited, 2017. • Διαχείριση της ασφάλειας πληροφοριών, Σ. Κάτσικας, Εκδόσεις Πολιτεία, 2015, ISBN 9789605464158 • Γκρίτζαλης Σ., Κάτσικας Σ., Γκρίτζαλης Δ., Ασφάλεια Δικτύων Υπολογιστών, Παπασωτηρίου, Αθήνα 2003. • Κάτσικας Σ., Γκρίτζαλης Δ., Γκρίτζαλης Σ. (επ. επιμ.), Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών, Αθήνα 2004. • Peltier T., Information Security Policies and Procedures, CRC Press, 1999.
α/α Διδακτικής Ενότητας	**4**
Τίτλος Διδακτικής Ενότητας	**Διαδικασίες Ασφάλειας**
Αναλυτική Περιγραφή Διδακτικής Ενότητας	• Ελεγχόμενη Πρόσβαση των Χρηστών στο Δίκτυο (Network Access Control) • Ελεγχόμενη Πρόσβαση Ιστότοπου (Website Access Control) • Διαδικασία Διαχείρισης Αλλαγών (Change Management Procedure) • Σχέδιο Συνέχισης Λειτουργίας (Business Continuity Plan) Παράδειγμα – μελέτη περίπτωσης
Διάρκεια (ώρες)	**3**
Εκπαιδευτικές τεχνικές (ενδεικτικά: εργαστήριο, μελέτη περίπτωσης, εργασία, άσκηση κ.ά.)	**Διάλεξη – Συζήτηση – Καταιγισμός Ιδεών – Ομάδες Εργασίας – Πρακτική Εξάσκηση**
Βασικό Εκπαιδευτικό Υλικό (όπως παρουσιάσεις διδασκόντων, ενότητες βιβλίων, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• CYBERSECURITY_ESDD_2021_enotita_4.pdf • Εκπαιδευτικό υλικό ΕΣΔΔΑ 2018, CYBERSECURITY.pdf
Ενδεικτικό Εκπαιδευτικό Υλικό (όπως βιβλία, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• Network Security Essentials: Applications and Standards (6th Edition), by William Stallings, Pearson Education Limited, 2017. • Διαχείριση της ασφάλειας πληροφοριών, Σ. Κάτσικας, Εκδόσεις Πολιτεία, 2015, ISBN 9789605464158 • Γκρίτζαλης Σ., Κάτσικας Σ., Γκρίτζαλης Δ., Ασφάλεια Δικτύων Υπολογιστών, Παπασωτηρίου, Αθήνα 2003. • Κάτσικας Σ., Γκρίτζαλης Δ., Γκρίτζαλης Σ. (επ. επιμ.), Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών, Αθήνα 2004.

	• Peltier T., Information Security Policies and Procedures, CRC Press, 1999.
α/α Διδακτικής Ενότητας	**5**
Τίτλος Διδακτικής Ενότητας	**Νομικά Θέματα**
Αναλυτική Περιγραφή Διδακτικής Ενότητας	• **Ασφάλεια Πληροφοριακών Συστημάτων, Δικτύων και Δεδομένων** • **Επιθέσεις κατά Συστημάτων Πληροφοριών** • **ENISA** • **Γενικός Κανονισμός Προσωπικών Δεδομένων** • **Αρμόδιοι φορείς και Αρχές** Παράδειγμα – μελέτη περίπτωσης
Διάρκεια (ώρες)	**3**
Εκπαιδευτικές τεχνικές (ενδεικτικά: εργαστήριο, μελέτη περίπτωσης, εργασία, άσκηση κ.ά.)	**Διάλεξη – Συζήτηση – Καταιγισμός Ιδεών – Ομάδες Εργασίας**
Βασικό Εκπαιδευτικό Υλικό (όπως παρουσιάσεις διδασκόντων, ενότητες βιβλίων, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• CYBERSECURITY_ESDD_2021_enotita_5.pdf • Εκπαιδευτικό υλικό ΕΣΔΔΑ, CYBERSECURITY.pdf
Ενδεικτικό Εκπαιδευτικό Υλικό (όπως βιβλία, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• Γερμανός, Γ. και Παπαθανασίου, Α. (2017). Νομοθεσία για το έγκλημα στον κυβερνοχώρο και την ψηφιακή εγκληματικότητα. Εκδόσεις Αντ. Ν. Σάκκουλα Ε.Ε. • Νόμος 4577/2018 (ΦΕΚ Α’ 199/3-12-2018) • Νόμος 4411/2016 (ΦΕΚ Α' 142/3-8-2016) • Νόμος 4070/2012 Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις • Νόμος 3979/2011 - (ΦΕΚ 138 Α/16-6-2011) • ΠΔ 25/2014 Ηλεκτρονικό Αρχείο και Ψηφιοποίηση Εγγράφων • Ευρωπαϊκός Κανονισμός 2016/679 (Γενικός Κανονισμός Προστασίας Δεδομένων) • Ευρωπαϊκός Κανονισμός eIDAS (ΕΕ) 910/2014 • ENISA: https://www.enisa.europa.eu/ • Cybersecurity Law: http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1119231507.html • Cybersecurity and Cyberwar: https://www.goodreads.com/book/show/16182409-cybersecurity-and-cyberwar • Introduction to Cyber-Warfare 1st Edition: https://www.elsevier.com/books/introduction-to-cyber-warfare/shakarian/978-0-12-407814-7?utm_source=publicity&utm_medium=pressrelease&utm_campaign=cybersecurity
α/α Διδακτικής Ενότητας	**6**

Τίτλος Διδακτικής Ενότητας	**Ασφάλεια Κοινωνικών Δικτύων**
Αναλυτική Περιγραφή Διδακτικής Ενότητας	• Κίνδυνοι ασφάλειας και ιδιωτικότητας στις εφαρμογές κοινωνικής δικτύωσης • Η περίπτωση του Facebook • Η περίπτωση του Twitter • Ορθή Χρήση Μέσων Κοινωνικής Δικτύωσης Παράδειγμα – μελέτη περίπτωσης
Διάρκεια (ώρες)	**3**
Εκπαιδευτικές τεχνικές (ενδεικτικά: εργαστήριο, μελέτη περίπτωσης, εργασία, άσκηση κ.ά.)	**Διάλεξη – Συζήτηση – Καταιγισμός Ιδεών – Ομάδες Εργασίας – Πρακτική Εξάσκηση**
Βασικό Εκπαιδευτικό Υλικό (όπως παρουσιάσεις διδασκόντων, ενότητες βιβλίων, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• CYBERSECURITY_ESDD_2021_enotita_6.pdf • Εκπαιδευτικό υλικό ΕΣΔΔΑ, CYBERSECURITY.pdf
Ενδεικτικό Εκπαιδευτικό Υλικό (όπως βιβλία, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• Network Security Essentials: Applications and Standards (6th Edition), by William Stallings, Pearson Education Limited, 2017. • Acquisti, A. and Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. Privacy Enhancing Technologies (PET) Lecture Notes in Computer Science, 4258:36–58. • ENISA Position Paper No.1 (2007). Security Issues and Recommendations for Online Social Networks. European Network and Information Security Agency. • McDowell, M. and Morda, D. (2011). Socializing Securely: Using Social Networking Services. Produced for United States Computer Emergency Readiness Team (US-CERT) by Carnegie Mellon University. • McCarthy, L., Watson, K. and Weldon-Siviy, D. (2011). Own Your Space: A Guide to Facebook Security. Facebook. • Dinerman, B. (2011). Social networking and security risks. GFI White Paper, GFI Software. • Facebook (2010). Facebook Privacy & Security Guide. Secure State and SocialMediaSecurity.com. http://socialmediasecurity.com/downloads/Facebook_Privacy_and_Security_Guide.pdf • Facebook (2012). Facebook Security Best Practices. Sophos. http://www.sophos.com/en-us/security-news-trends/best-practices/facebook.aspx • Huina Mao, Xin Shuai, Apu Kapadia, (2011). Loose Tweets: An Analysis of Privacy Leaks on Twitter. Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, WPES'11, pp. 1-12. • Humphreys, L., Gill, P. and Krishnamurthy, B. (2010). How much is too much? Privacy issues on Twitter. In Conference of International Communication Association, Singapore. • Meeder, B., Tam, J.. Kelley, P. G. and Cranor, L. F. (2010). RT@ IWantPrivacy: Widespread violation of privacy

	settings in the Twitter social network. In Web 2.0 Privacy and Security Workshop, IEEE Symposium on Security and Privacy. • Java, A., Song, X., Finin, T. and Tseng, B. (2007). Why we twitter: understanding microblogging usage and communities. WebKDD/SNA-KDD '07: Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 workshop on Web mining and social network analysis. New York, NY, USA: ACM, pp. 56–65. • Krishnamurthy, B., Gill, P. and Arlitt, M. (2008). A few chirps about twitter. WOSP '08: Proceedings of the first workshop on Online social networks. New York, NY, USA: ACM, pp. 19–24. • Griery, C., Thomas, K., Paxsony V., and Zhang, M. (2010). @spam: The Underground on 140 Characters or Less. Proceedings of the 17th ACM conference on Computer and communications security, pp. 27-37. • Benevenuto, F., Magno, G., Rodrigues, T., and Almeida, V. (2010), Detecting Spammers on Twitter. Seventh annual Collaboration, Electronic messaging, AntiAbuse and Spam Conference CEAS. • Irani, D., Webb, S., Pu, C. and Li, K. (2010). Study of TrendStuffing on Twitter through Text Classification. Seventh annual Collaboration, Electronic messaging, AntiAbuse and Spam Conference CEAS. • De Cristofaro, E., Soriente, C., Tsudik, G., Williams, A. (2012) Hummingbird: privacy at the time of Twitter. 33th IEEE Symposium on Security and Privacy.
α/α Διδακτικής Ενότητας	**7**
Τίτλος Διδακτικής Ενότητας	**Κυβερνοεπιθέσεις Ευρείας Κλίμακας**
Αναλυτική Περιγραφή Διδακτικής Ενότητας	• Η Περίπτωση του Ιομορφικού Λογισμικού Flame • Ανάλυση Χαρακτηριστικών και Ταξινόμηση • Συμπεράσματα Άσκηση
Διάρκεια (ώρες)	**3**
Εκπαιδευτικές τεχνικές (ενδεικτικά: εργαστήριο, μελέτη περίπτωσης, εργασία, άσκηση κ.ά.)	**Διάλεξη – Συζήτηση – Καταιγισμός Ιδεών – Ομάδες Εργασίας**
Βασικό Εκπαιδευτικό Υλικό (όπως παρουσιάσεις διδασκόντων, ενότητες βιβλίων, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• CYBERSECURITY_ESDD_2021_enotita_7.pdf • Εκπαιδευτικό υλικό ΕΣΔΔΑ, CYBERSECURITY.pdf
Ενδεικτικό Εκπαιδευτικό Υλικό (όπως βιβλία, μελέτες περίπτωσης, άρθρα, διαδικτυακοί τόποι, κανονιστικά κείμενα, κ.ά.)	• Bencsáth B., Pék G., Buttyán L., Félegyházi M. (2012). *The Cousins of Stuxnet: Duqu, Flame, and Gauss*. Future Internet, 4(4), pp.971-1003.

- Munro K. (2012). *Deconstructing Flame: the limitations of traditional defenses*. Elsevier, Computer Fraud & Security Volume 2012, Issue 10, pp. 8–11.
- Bit9 Threat Advisor (2012). *Don't get burned by Flame*. Vol. 1, No. 3.
- Boothby W.H., von Heinegg W.H., Michael J.B., Schmitt M.N., Wingfield T.C. (2012). *When Is a Cyberattack a Use of Force or an Armed Attack?*. IEEE Computer, Volume 45, Issue 8, pp. 82-84.
- Marks P. (2012). *Why we may never know who created Flame virus*. New Scientist, Volume 214, Issue 2868, pp. 24.
- Jolley J. D. (2012). *Article 2(4) and Cyber Warfare: How Do Old Rules Control the Brave New World?*. Social Science Electronic Publishing, Inc.
- Goyal R., Sharma S., Bevinakoppa S., Watters P. (2012). *Obfuscation of Stuxnet and Flame Malware*. Proceedings of the 3rd International conference on Applied Informatics and Computing Theory (AICT '12). Latest Trends in Applied Informatics and Computing, Barcelona, Spain.
- Symantec Official Blog (2012). *W32.Flamer: Enormous Data Collection*. http://www.symantec.com/connect/blogs/w32flamer-enormous-data-collection
- Symantec Official Blog (2012). *Painting a Picture of W32.Flamer*, http://www.symantec.com/connect/blogs/painting-picture-w32flamer
- Symantec Official Blog (2012) "W32.Flamer: Microsoft Windows Update Man-in-the-Middle", http://www.symantec.com/connect/blogs/w32flamer-microsoft-windows-update-man-middle
- Symantec Security Response (2012). *W32.Flamer*, http://www.symantec.com/security_response/writeup.jsp?docid=2012-052811-0308-99
- sKyWIper Analysis Team (2012). *sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks*. Budapest University of Technology and Economics, Department of Telecommunications, v1.05.
- Gostev A. (2012a), "The Flame: Questions and Answers", Kaspersky Lab, http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers
- Gostev, A. (2012b). *Back to Stuxnet: the missing link.* Kaspersky Lab, https://www.securelist.com/en/blog/208193568/Back_to_Stuxnet_the_missing_link
- Sotirov A. (2012). *Analyzing the MD5 Collision in Flame*, https://speakerdeck.com/asotirov/analyzing-the-md5-collision-in-flame
- Stevens M. (2012). *Attacks on Hash Functions and Applications.* Mathematical Institute, Leiden University.

	• Sotirov A., Stevens M., Appelbaum J., Lenstra, A., Molnar D., Osvik, D.A., De Weger B. (2008). *MD5 considered harmful today - Creating a rogue CA certificate.* Presented at 25th Chaos Communications Congress, Berlin, Germany. • Stevens M. (2012). *Technical Background on the Flame Collision Attack*". CWI (Centrum Wiskunde & Informatica) News. • Antiy Labs (2012). *Analysis Report on Flame Worm Samples.* Version 1.3.0. • Symantec Security Response (2012). *Have I Got Newsforyou: Analysis of Flamer C&C Server*.

Ο Υπεύθυνος
του εκπαιδευτικού υλικού