Силабус курсу:

ОСНОВИ КОМ'ПЮТЕРНОЇ КРИМІНАЛІСТИКИ

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Ступінь вищої освіти:	бакалавр
Спеціальність:	123 «Комп'ютерна інженерія»
Рік підготовки:	4
Семестр викладання:	осінній
Кількість кредитів ЄКТС:	5
Мова(-и) викладання:	українська
Вид семестрового контролю	залік

Автор курсу та лектор:

автор курсу, лектор Критська Я.О., автор курсу к.т.н., доцент Білобородова Т.О.
вчений ступінь, вчене звання, прізвище, ім'я та по-батькові

лектор - ст. викладач кафедри комп'ютерних наук та інженерії
посада

krytska@snu.edu.ua | - | Skype: YA Kritska | 405/401 НК, за розкладом
електронна адреса | телефон | месенджер | консультації

Викладач лабораторних та практичнихзанять:*

Критська Яна Олександрівна
вчений ступінь, вчене звання, прізвище, ім'я та по-батькові

ст. викладач кафедри комп'ютерних наук та інженерії
посада

krytska@snu.edu.ua | - | Skype: YA Kritska | 407 НК, за розкладом
електронна адреса | телефон | месенджер | консультації

Анотація навчального курсу

Цілі вивчення курсу: Наведені в курсі матеріали спрямовані на формування у студентів знань і навичок в питаннях щодо теоретичних основ і методів надання доказів впливу комп'ютерної інформації.

Метою лекційних занять за дисципліною «Основи комп'ютерної криміналістики є забезпечення достатнього рівня теоретичних знань, необхідних для розуміння процесів комп'ютерної криміналістики.

Метою практичних занять за дисципліною є формування здатності і готовності здобувача до використання набутих знань та умінь на практиці, формування самостійного застосування методів збору, обробки, збереження інформаційних доказів.

Метою лабораторних робіт за дисципліною є дослідження цифрових доказів, вивчення інструментів і методів дослідження комп'ютерної інформації, різних типи атак і вразливостей, алгоритмів безпеки, способів їх використання та рекомендації щодо підвищення безпеки інформаційних технологій.

Метою самостійної роботи за дисципліною є систематизація і закріплення отриманих теоретичних знань і практичних навичок здобувачів вищої освіти; формування умінь виявляти вразливості операційних систем, мережних протоколів, сайтів, програмних засобів, додатків; формувати алгоритми забезпечення безпеки, рекомендації для підвищення захищеності комп'ютерних даних.

Курс може бути корисним студентам за спеціальностями в галузі «12. Інформаційні технології», а також майбутнім фахівцям, що планують працевлаштування на підприємства та фірми діяльність яких пов'язана з оцінкою комп'ютерної криміналістики та створенні інформаційних систем кібербезпеки.

Результати навчання: Знати: методи збору, обробки, збереження інформаційних доказів комп'ютерних правопорушень в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі аналізу, синтезу та проектування інформаційних технологій за галузями.

Вміти: ефективно використовувати методи збору, обробки, збереження доказів правопорушень в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі аналізу, синтезу та проектування інформаційних технологій за галузями.

	Призначено для інженерів, які займаються розробленням та впровадженням систем захисту інформації веб-додатків, сервісів та мереж, для груп верифікації, для веб-розробників і фахівців у галузі оцінювання якості та безпеки веб-додатків, для магістрів і аспірантів університетів, які навчаються за напрямами інформаційної безпеки, комп'ютерних наук, комп'ютерної та програмної інженерії, а також для викладачів відповідних курсів.
Передумови до початку вивчення:	Базові знання зі створення системних та прикладних програм, криптографічних методів захисту інформації, дискретної математики, чисельних методів, теорії чисел.

Мета курсу (набуті компетентності)

В наслідок вивчення даного навчального курсу здобувач вищої освіти набуде наступних компетентностей:

1. Навички обґрунтовування та розробки тактики оперативно- дослідних дій, пов'язаних з комп'ютерною інформацією.
2. Здатність вибору методів і інструментів для збору і вивчення доказів комп'ютерних злочинів.
3. Здатність визначення підходів для встановлення криміналістичних характеристик правопорушень, пов'язаних з комп'ютерною інформацією.
4. Здатність розв'язування теоретичні і прикладні задачі для проникнення в середину комп'ютерних систем та виявлення порушення прав інтелектуальної власності, інформації щодо комерційних чи персональних даних об'єктів комп'ютерної інформації.
5. Здатність застосування навичків захисту інформації в галузі інформаційних технологій, системах підтримки рішень при техногенного оцінки ризику.

Структура курсу

№	Тема	Години (Л/ЛБ/ПЗ)	Стислий зміст	Інструменти і завдання
1.	Введення в основи курсу. Тенденції і перспективи комп'ютерної криміналістики	4/2/4	Основні поняття, терміни і визначники. Задачі, методи і форми комп'ютерної криміналістики.	Участь в обговоренні Тести Індивідуальні завдання
2.	Пріоритетність та етапи розслідування. Контрфорнзика	4/2/4	Спеціальні технічні засоби. Пріоритетність розслідування правопорушень. Захисні антикриміналістичні засоби.	Участь в обговоренні Тести Індивідуальні завдання
3.	Комп'ютерні правопорушення	4/2/4	Криміналістична характеристика. Види правопорушень: онлайн-шахрайство, образи в мережі, DoS-атаки, дефейс, шкідливі ПО, кардерство, шахрайство з трафіком, порушення авторських прав, фішинг, кіберсквоттинг.	Участь в обговоренні Тести Індивідуальні завдання
4.	Операційно - пошукові заходи	4/2/4	Взаємодії та дослідження правопорушень (перехоплення, статистичні дослідження даних, вибіркове перехоплення). Дослідження лагів (системних та мейл-серверу електронної пошти). Встановлення приналежності IP-адреси, доменного ім'я, адреси електронної пошти. Кейлогери	Участь в обговоренні Тести Індивідуальні завдання
5.	Слідчі дії. Дослідження правопорушень	4/2/4	Порядок проведення слідчих дій, нормативні акти. Загальні правила вилучення комп'ютерної техніки при обшуку і їх особливості. Тактика дослідження правопорушень (тактика обшуку, лог-файли й докази сили логів. Дані з коротким терміном існування.	Участь в обговоренні Тести Індивідуальні завдання
6.	Завірення контенту	4/2/4	Особливості завірення контенту. Види розміщення контенту (веб-сайт, телеконференції, файлобмінники, інше)	Участь в обговоренні Тести

№	Тема	Години (Л/ЛБ/ПЗ)	Стислий зміст	Інструменти і завдання
				Індивідуальні завдання
7.	Комп'ютерно-технічна експертиза	4/2/4	Місці і роль комп'ютерно-технічної експертизи. Проблеми та методи КТЕ. Типи носіїв. Зашифровані дані. Експертні засоби і інструменти для вивчення і реконструкції даних. Дослідження програм і документів.	Участь в обговоренні Тести Індивідуальні завдання

Рекомендована література

1. Damn Vulnerable Web Application (DVWA). http://www.dvwa.co.uk/
2. Damn Vulnerable Linux. https://distrowatch.com/dvl
3. OWASP WebGoat Project.
https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
4. Статистика уязвимостей веб-приложений (2013 г.) – Positive Technologies https://www.ptsecurity.com/ww-en/
5. Owasp Top 10: The Top 10 Most Critical Web Application Security Threats: Enhanced with Text Analytics and Content by Pagekicker Robot Phil 73 // Createspace. – 2014. – 54 p.
6. OWASP Testing Guide 4.0. https://www.owasp.org/images/1/19/OTGv4.pdf
7. How to Use Wireshark to Capture, Filter and Inspect Packets. https://www.howtogeek.com/104278/how-to-use-wireshark-to-capturefilter-
and-inspect-packets/
8. Burp Suite Tutorial – Web Application Penetration Testing (Part 1). https://www.pentestgeek.com/web-applications/burp-suitetutorial-1
9. Man-in-the-middle attack. https://www.owasp.org/index.php/Man-in-the-middle_attack
10. SQL Injection. https://www.owasp.org/index.php/SQL_Injection
11. Justine Clarke. SQL Injection Attacks and Defense. / Syngress Publishing, Inc., 2009. – 576 p.
12. А.Г. Тецкий. Исследование методов получения содержимого базы данных с помощью SQL-инъекций. – Открытые информационные и компьютерные интегрированные технологии: сб. науч. тр. – Х. : Нац. аэрокосм. ун-т «Харк. авиац. ин-т», 2014. – Вып. 66. – с. 188-191.
13. Sqlmap. http://sqlmap.org/
14. NT Web Technology Vulnerabilities. http://phrack.org/issues/54/8.html
15. Cross-site Scripting (XSS). https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
16. XSSer: Cross Site "Scripter". https://xsser.03c8.net /
17. Metasploit Framework User Guide.
http://cs.uccs.edu/~cs591/metasploit/users_guide3_1.pdf
18. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni. Metasploit. – 2011. – 328 p.
19. Penetration Testing Software | Metasploit. https://www.metasploit.com/
20. Unrestricted File Upload. https://www.owasp.org/index.php/Unrestricted_File_Upload
21. Nmap: the Network Mapper - Free Security Scanner. https://nmap.org/
22. Secunia Research Community.
https://secuniaresearch.flexerasoftware.com/community/research/
23. OSVDB | Everything is Vulnerable. https://blog.osvdb.org/ 24. National Vulnerability Database. https://nvd.nist.gov/
25. Common Vulnerabilities and Exposures. https://cve.mitre.org/
26. Web Application Firewall.
https://www.owasp.org/index.php/Web_Application_Firewall
27. Ric Messier. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems / Apress, 2016. – 115 p.
28. Ron Lepofsky. The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web / Apress, 2014. – 232 p.
29. Alienin O. I., Gabinet A. V., Rokovyi O. P., Stirenko S. G., Illiashenko O.A., Strielkina A. A., Methods and tools for technical auditing of information security of

computer systems and networks. Practice. / Edited by Kharchenko V. S. – Department of Education and Science of Ukraine, National Aerospace University named after N. E. Zhukovsky “KhAI”, 2017. – 136 p.

Методичне забезпечення

1. О. І. Алєнін, А. В. Габінет, О. П. Роковий, С. Г. Стіренко, О. О. Ілляшенко, А. А. Стрєлкіна Методи та засоби технічного аудиту інформаційної безпеки комп’ютерних систем та мереж. Практикум / под ред. В.С. Харченко – Министерство освіти та науки України, Національний аэрокосмічний університет ім. М .Є. Жуковського «ХАІ». 2017. – 136 с.

Оцінювання курсу

За повністю виконані завдання студент може отримати визначену кількість балів:

Інструменти і завдання	Кількість балів
Участь в обговоренні	10
Тести	25
Виконання лабораторних і практичних робіт	35
Залік	30
Разом	**100**

Шкала оцінювання студентів

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	F	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

Політика курсу

Плагіат та академічна доброчесність:	Студент може пройти певні онлайн-курси, які пов'язані з темами дисципліни, на онлайн-платформах. При поданні документу про проходження курсу студенту можуть бути перезараховані певні теми курсу та нараховані бали за завдання. Під час виконання завдань студент має дотримуватись політики академічної доброчесності. Запозичення мають бути оформлені відповідними посиланнями. Списування є забороненим.
Завдання і заняття:	Всі завдання, передбачені програмою курсу мають бути виконані своєчасно і оцінені в спосіб, зазначений вище. Аудиторні заняття мають відвідуватись регулярно. Пропущені заняття (з будь-яких причин) мають бути відпрацьовані з отриманням відповідної оцінки не пізніше останнього тижня поточного семестру. В разі поважної причини (хвороба, академічна мобільність тощо) терміни можуть бути збільшені за письмовим дозволом декана.
Поведінка в аудиторії:	На заняття студенти вчасно приходять до аудиторії відповідно до діючого розкладу та обов’язково мають дотримуватися вимог техніки безпеки. Під час занять студенти: – не вживають їжу та жувальну гумку; – не залишають аудиторію без дозволу викладача; – не заважають викладачу проводити заняття. Під час контролю знань студенти: – є підготовленими відповідно до вимог даного курсу; – розраховують тільки на власні знання (не шукають інші джерела інформації або «допомоги» інших осіб); – не заважають іншим; – виконують усі вимоги викладачів щодо контролю знань.