МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
М.В. Афанасьєв

ЗАХИСТ СИСТЕМ ЕЛЕКТРОННОЇ КОМЕРЦІЇ ТА МУЛЬТИСЕРВІСНИХ СИСТЕМ

робоча програма навчальної дисципліни

Галузь знань	**12 “ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ”**
Спеціальність	**125 “КІБЕРБЕЗПЕКА”**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**“КІБЕРБЕЗПЕКА”**

Вид дисципліни	**базова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри *кібербезпеки та інформаційних технологій* Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця
2019

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 6 від 10.12.2019 р.
Розробник(-и):

Погасій, к.е.н., доцент кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

1. Вступ

Програма вивчення навчальної дисципліни "Захист систем електронної комерції та мультисервісних систем" складена відповідно до освітньої програми підготовки бакалаврів зі спеціальності 125 "Кібербезпека".

Анотація навчальної дисципліни: Дисципліна “Захист систем електронної комерції та мультисервісних систем” є базовою навчально дисципліною за спеціальністю “Кібербезпека”.

Важливо в системі економічної безпеки електронної комерції визначити, класифікувати і ранжувати загрози. Оскільки відносини у сфері електронної комерції відзначаються великою різноманітністю, включають різних учасників, мають різні характеристики і потребу різного ступеня захищеності, тому й загрози їхній безпеці різноманітні.

Предметом навчальної дисципліни є вивчення навчальної дисципліни є теоретичні концепції та методології, принципи функціонування, захисту даних, вибору і практичної реалізації захисту в системах електронної комерції та мультисервісних системах.

Метою навчальної дисципліни є формування у студентів знань про основні типи атак на веб-додатки та веб-сервіси і методів, їх запобігання. Знання, отримані в результаті вивчення цієї дисципліни, дозволять студентам не допускати стандартних помилок в області безпеки при роботі з системам електронної комерції.

Головне завдання курсу – освоєння принципів використання програмного забезпечення для тестування та виявлення вразливостей веб-додатків та веб-сервісів та створення систем захисту від виявлених вразливостей, запобігання шляхів несанкціонованого доступу (НСД) до даних в мультисервісних системах та системах електроної комерції; вживання заходів протидії проникненню шкідливого програмного забезпечення та відновлення працездатності мультисервісних систем після знешкодження загроз.

Курс	**1**	
Семестр	**2**	
Кількість кредитів ECTS	**5**	
Аудиторні навчальні заняття	**лекції**	**36**
	лабораторні	**38**
Самостійна робота		**76**
Форма підсумкового контролю	**Залік**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Основи побудови та захисту сучасних операційних систем	Корпоративні мережі та системи доступу
Організаційне забезпечення захисту інформації	Безпека та аудит бездротових та рухомих мереж
Комплексні системи захисту інформації	Основи планування та адміністрування служб доступу до інформаційних ресурсів

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатність проводити аналіз особливостей діяльності організації та використання в ній мультисервісних систем з метою визначення інформаційно-технологічних ресурсів, що підлягають захисту;	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
Здатність брати участь у формуванні політики інформаційної безпеки організації і контролювати ефективність її реалізації;.	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (ас) організації (підприємства) відповідно до вимог нормативно-правових документів;
Здатність формувати комплекс заходів (правила, процедури, практичних прийомів, керівних принципів, методи, засоби) для забезпечення інформаційної безпеки мультисервісних систем	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (ас) організації (підприємства) відповідно до вимог нормативно-правових документів;

3. Програма навчальної дисципліни

Змістовний модуль 1. Основи захисту веб-додатків та веб-сервісів.

Тема 1 Вступ. Термінологія, статистика атак на web-ресурси.

Публічність web-додатків як один з факторів підвищеної уваги зловмисників до web-ресурсів. Атака «зловживання функціональністю».

Атаки «Груба сила» і «Переповнення буфера». Атака «Відмова в обслуговуванні»: класифікація методів, способи захисту.

Тема 2. Атака «Міжсайтовий скриптинг»

Атака «ін'єкція команд в протоколи електронної пошти». Поняття LDAP репозіторія (Lightweight Directory Access Protocol), методи атак на LDAP

Змістовний модуль 2. Основи криптографічного захисту веб-додатків та веб-сервісів.

Тема 3. Атака на web-сервер

Загальна схема функціонування систем з відкритими ключами. Загальна схема функціонування систем з відкритими ключами. Захист паролів на Web-серверах

Тема 4. Безпека адрес

Перевірка web-додатків на захист. Web Захист.

Теми лабораторних робіт:

Лабораторна робота №1. Дослідження методів захисту Honeypot,

Лабораторна робота №2. Дослідження методів сканування Nmap

Лабораторна робота №3. Дослідження процесів побудови мультисервісної системи

Лабораторна робота №4. Дослідження процесів встановлення CMS

Лабораторна робота №5. Дослідження load testing та stress testing веб-серверів

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, семінарські, практичні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних, лабораторних занять і оцінюється сумою набраних балів;

модульний контроль, що проводиться у формі поточних контрольних робіт як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лабораторних занять проводиться за такими критеріями:

- продемонструвати навички проводити аналіз особливостей діяльності організації та використання в ній мультисервісних систем з метою визначення інформаційно-технологічних ресурсів, що підлягають захисту;

- розробити деякі положення шодо формуванні політики інформаційної безпеки організації і контролювати ефективність її реалізації;.

- впровадити комплекс заходів (правила, процедури, практичних прийомів, керівних принципів, методи, засоби) для забезпечення інформаційної безпеки мультисервісних систем.

- здійснити комплекс заходів щодо захисту програм та інформації, що

обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

- реалізувати комплексні системи захисту інформації в автоматизованих системах (ас) організації (підприємства) відповідно до вимог нормативно-правових документів.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового заліку за накопичуваними балами, що були отримані протягом навчального семестру,.

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами навчальної дисципліни розраховується з урахуванням балів, отриманих під поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: “60 і більше балів – зараховано”, “59 і менше балів – не зараховано” та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Розподіл балів за тижнями

Теми змістового модуля			Лекційні заняття	Лабораторні заняття	Письмова контрол	Експрес опитування	Усього
Змістовний модуль	Тема	Тиждень					
Змістовий модуль 1.	Тема 1	1 Тиждень	2				2
		2 Тиждень	2				2
		3 Тиждень	2				2
		4 Тиждень	2	8			10
		5 Тиждень	2				2
		6 Тиждень	2	8			10
	Тема 2	7 Тиждень	2			4	2
		8 Тиждень	2		10		12
		9 Тиждень	2				2
		10 Тиждень	2	8			10
Змістовий модуль 2.	Тема 3	11 Тиждень	2				2
		12 Тиждень	2				2
		13 Тиждень	2	8			10
	Тема 4	14 Тиждень	2			4	2
		15 Тиждень	2		10		12
		16 Тиждень	2	8			10
Усього			32	40	20	8	100

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	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	не зараховано
1 – 34	F		

5. Рекомендована література

5.1 Основна

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-suite-tutorial-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.

5.2 Додаткова

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

5.3 Інформаційні ресурси в Інтернеті

18.Penetration Testing Software | Metasploit. https://www.metasploit.com/

19.Unrestricted File Upload. https://www.owasp.org/index.php/Unrestricted_File_Upload

20.Nmap: the Network Mapper - Free Security Scanner. https://nmap.org/

21.Secunia Research Community https://secuniaresearch.flexerasoftware.com/community/research/

22.OSVDB | Everything is Vulnerable. https://blog.osvdb.org/

23.National Vulnerability Database. https://nvd.nist.gov/

24.Common Vulnerabilities and Exposures. https://cve.mitre.org/

25.Web Application Firewall. https://www.owasp.org/index.php/Web_Application_Firewall

26 Сайт дистанційного навчання ХНЕУ ім. С. Кузнеця навчальної дисципліни “Захист систем електронної комерції та мультисервісних систем” https://pns.hneu.edu.ua/course/view.php?id=5240.