МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"**ЗАТВЕРДЖУЮ**"
Заступник керівника
(проректор з науково-педагогічної роботи)

_____

"____"_____ 20_____року

ЗАХИСТ СИСТЕМ ЕЛЕКТРОННОЇ КОМЕРЦІЇ ТА МУЛЬТИСЕРВІСНИХ СИСТЕМ

Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	

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

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

Харків
ХНЕУ ім. С. Кузнеця
2018

ЗАТВЕРДЖЕНО
на засіданні кафедри Кібербезпеки та інформаційних технологій
Протокол № Х від ___._____.2018 р.

Розробник:
Шматко О.В., к.т.н., доц. кафедри КІС

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри
2018/2019			

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”. Вона викладається у шостому семестрі бакалаврату в обсязі 150 год.(5 кредитів ECTS), зокрема: лекції – 36 год., лабораторні – 38 год., самостійна робота – 74 год, консультації – 4 год. У курсі передбачено два змістових модулі та одна модульна контрольна робота. Завершується дисципліна заліком.

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 вебдодатків 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**
	семінарські, практичні	**-**
	лабораторні	**38**
Самостійна робота		**74**
Форма підсумкового контролю	**Залік**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	**Наступні дисципліни**
ОСНОВИ ПОБУДОВИ ТА ЗАХИСТУ СУЧАСНИХ ОПЕРАЦІНЙИХ 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 ІНФОРМАЦІНИХ 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

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, практичних, семінарських, лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

модульний контроль, що проводиться у формі колоквіуму 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;

підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час семінарських, практичних і лабораторних занять та виконання індивідуальних завдань проводиться за такими критеріями:

розуміння, ступінь засвоєння теорії та методології проблем, що розглядаються; ступінь засвоєння фактичного матеріалу навчальної дисципліни; ознайомлення з рекомендованою літературою, а також із сучасною літературою з питань, що розглядаються; вміння поєднувати теорію з практикою при розгляді виробничих ситуацій, розв'язанні задач, проведенні розрахунків у процесі виконання індивідуальних завдань та завдань, винесених на розгляд в аудиторії; логіка, структура, стиль викладу матеріалу в письмових роботах і при виступах в аудиторії, вміння обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки; арифметична правильність виконання індивідуального та комплексного розрахункового завдання; здатність проводити критичну та не-

залежну оцінку певних проблемних питань; вміння пояснювати альтернативні погляди та наявність власної точки зору, позиції на певне проблемне питання; застосування аналітичних підходів; якість і чіткість викладення міркувань; логіка, структуризація та обґрунтованість висновків щодо конкретної проблеми; самостійність виконання роботи; грамотність подачі матеріалу; використання методів порівняння, узагальнення понять та явищ; оформлення роботи.

Загальними критеріями, за якими здійснюється оцінювання позааудиторної самостійної роботи студентів, є: глибина і міцність знань, рівень мислення, вміння систематизувати знання за окремими темами, вміння робити обґрунтовані висновки, володіння категорійним апаратом, навички і прийоми виконання практичних завдань, вміння знаходити необхідну інформацію, здійснювати її систематизацію та обробку, самореалізація на практичних та семінарських заняттях.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 5 практичних ситуацій (два стереотипних, два діагностичних та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час 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
(вказати засоби оцінювання згідно з технологічною картою)

Теми змістового модуля			Лекційні заняття	Практичні заняття	Лабораторні заняття	Семінарські заняття	Перевірка есе	Презентація	Експрес-опитування	Тестування	Письмова контрольна робота	Колоквіум	Усього
Змістовний модуль	Тема	Тиждень											
Змістовий модуль 1.	1	1	1										1
		2	1										1
		3	1										1
		4	1		8								9
		5	1										1
		6	1		4								5
	2	7	1										1
		8	1								8		9
		9	1										1
		10	1		8								9

Змістовий модуль 2.	3	11	1										1
		12	1										1
		13	1		8								1
	4	14	1										1
		15	1										1
		16	1		8								9
	Залік												40
Усього													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