МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

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

ВЕБ-БЕЗПЕКА

робоча програма навчальної дисципліни

Галузь знань	**12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність	**125 "КІБЕРБЕЗПЕКА"**
Освітній рівень	**другий (магістерський)**
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):
Корольов Р.В., к.т.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

Анотація навчальної дисципліни:

Подано тематичний план навчальної дисципліни й її змістовність за модулями та темами, вміщено плани лекцій і лабораторних занять, матеріал щодо закріплення знань (завдання для самостійної роботи, контрольні запитання), методичні рекомендації та оцінювання знань студентів. Захист веб-ресурсів залишається одним із важливих напрямків інформаційної безпеки. Щороку кількість веб-ресурсів збільшується, зростає також кількість конфіденційної інформації, яка локалізується на серверах віддаленого доступу (особливо із використанням хмарних технологій).

У результаті цього зростають не тільки кількість атак на веб-ресурси, але й економічні наслідки таких атак. Вразливість веб-ресурсів до атак отримала політичний вимір унаслідок як поширення гібридних війн у світі, так і зростання терористичних загроз.

Таким чином вивчення методів і систем захисту веб-ресурсів від атак залишається актуальною проблемою, особливо з урахуванням постійного вдосконалення методів та інструментів атак і появи методів та інструментів.

Мета навчальної дисципліни: метою дисципліни "Веб-безпека" є формування теоретичних знань та практичних умінь у сфері забезпечення безпеки веб-ресурсів, їх інформаційної та кібернетичної безпеки.

Курс	**1**	
Семестр	**1**	
Кількість кредитів ECTS	**3**	
Аудиторні навчальні заняття	**лекції**	**12**
	семінарські, практичні	**–**
	лабораторні	**28**
Самостійна робота		**50**
Форма підсумкового контролю	**екзамен**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Забезпечення інформаційної безпеки	Дипломна робота
Безпека в інформаційно-комунікаційних системах	

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, безпеки інформаційних технологій (в т.ч. хмарних технологій та додатків), а також безпеки бізнес/операційних процесів з метою забезпечення функціонування інформаційно-комунікаційних систем згідно встановленої стратегії і політики	планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність

Компетентності	Результати навчання
інформаційної безпеки та/або кібербезпеки організації.	
Здатність розробляти та впроваджувати методи і заходи протидії кіберінцидентам, а також здійснювати процедури управління, контролю та розслідування, надавати рекомендації щодо попередження та аналізу кіберінцидентів.	проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо)

3. Програма навчальної дисципліни

Змістовий модуль 1. Реалізація методів захисту в протоколах обміну інформацією.

Тема 1. Протоколи HTTP та SOAP.

Протокол передачі гіпертексту. HTTP-запити та відповіді, методи та повідомлення. Кукі. HTTPS (протокол передачі гіпертексту через захищені сокети). Протокол SSL (Secure Sockets Layer). Використання простого протоколу доступу до об'єктів (SOAP).

Тема 2 . Захист конфіденційності клієнт-серверного додатка завдяки POP, SMTP, IMAP.

Використання протоколу простого доступу до об’єктів (SOAP). Протокол SMTP (Simple Mail Transfer Protocol). Протокол поштового відділення (POP3). Протокол доступу до Інтернету (IMAP).

Змістовий модуль 2. Веб-атаки.

Тема 3. Архітектура веб-систем. Об’єкти захисту/атаки. Аутентифікація та авторизація.

Архітектура веб-систем і веб-додатків. Об’єкти захисту/атаки. Класифікація веб-атак (уразливості). Груба сила (Brute Force). Недостатня аутентифікація. Недостатнє відновлення пароля (перевірка слабкого відновлення пароля).

Тема 4. Атаки на стороні клієнта.

Перехресні сценарії (XSS). Сценарії крос-кадрів (XFS) або iframe-ін’єкція. Підробка запитів на місцях, CSRF. Зловживання JSON.

Тема 5. Розкриття інформації. Логічні атаки.

Поняття LDAP-ін’єкція, SQL-ін’єкція, SSI-ін’єкція, XPath-ін’єкція. Індексування каталогів.

Змістовий модуль 3. Розробка захищених об’єктів. Проекти OWASP.

Тема 6. Методології розробки захищених сайтів. Проекти OWASP. Огляд керівництва по тестуванню OWASP. Аудит безпеки веб-сайтів (WSSA)

Проект тестування OWASP. Принципи тестування. Пояснення техніки тестування. Виведення вимог до тестування безпеки. Тести безпеки, інтегровані в робочі процеси розробки та тестування. Аналіз і звітність тестових даних безпеки. Інструменти тестування. Основні поняття аудиту веб-додатків. Методика організації та проведення аудиту веб-додатків.

Лабораторні роботи:

Лабораторна робота 1. Командні ін'єкції.Цифрова SQL-ін'єкція. Підробний спуфінг.

Лабораторна робота 2. XPath ін'єкція. Backdoor атака.Сліпе впровадження операторів SQL (BlindSQL Injection).

Лабораторна робота 3. Міжсайтовий скріптинг (XSS).

Лабораторна робота 4. Безпека AJAX.

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні 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 (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 лабораторних занять та виконання індивідуальних завдань проводиться за такими критеріями:

- здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, безпеки інформаційних технологій (в т.ч. хмарних технологій та додатків), а також безпеки бізнес/операційних процесів з метою забезпечення функціонування інформаційно-комунікаційних систем згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

- здатність розробляти та впроваджувати методи і заходи протидії кіберінцидентам, а також здійснювати процедури управління, контролю та розслідування, надавати рекомендації щодо попередження та аналізу кіберінцидентів.

Результати навчання:

- планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність

- проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо).

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 3 практичних ситуацій (одне стереотипне, одне діагностичне 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	Захист лабораторних робіт	Контрольна робота	Екзамен	Усього
	1	**Тема 1**	10 тиждень	2				2
		Тема 2	11 тиждень	2	10			12
	2	**Тема 3**	12 тиждень	2				2
		Тема 4	13 тиждень	2	10			12
		Тема 5	14 тиждень	2				2
	3	**Тема 6**	15 тиждень	2	10			12
			16 тиждень			8		8
			17 тиждень		10			10
	ЕКЗАМЕН						40	40
Усього				12	40	8	40	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. Gerardus Blokdyk. OWASP: Third Edition, 2018.
2. Binkly Schiller. Botnets: The Killer Web App.
3. Andres Andre. Professional Pen Testing for Web Applications.
4. Michael Hartl, Aurelius Prochazka. RailsSpace: Building a Social Networking Website with Ruby on Rails.
5. Dafydd Stuttard, Marcus Pinto. The Web Application Hacker’s Handbook.

5.2. Інформаційні ресурси в Інтернеті

6. https://www.owasp.org/index.php/Category:OWASP_Books
7. https://load-knigi.org/5373-piter-yavorski-osnovy-veb-hakinga-bolee-30-primerov-uyazvimostey-2016-pdf.html
8. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “Веб-безпека“ https://pns.hneu.edu.ua/course/view.php?id=5660