Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та управління

Кафедра інформаційної та кібернетичної безпеки

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ О.Б. Жильцов
«_31_» ____01_____ 2019 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ БЕЗПЕКИ WEB-РЕСУРСІВ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	другого (магістерського)
освітньої програми	125.00.02 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 2949/19
(підпис) (прізвище, ініціали)
«___» _____ 2019 р.

Київ – 2019

Розробники:

Соколов Володимир Юрійович, старший викладач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладачі:

Соколов Володимир Юрійович, старший викладач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки

Протокол від №1 від 16.01.2019 р.

Завідувач кафедри _____ В.Л. Бурячок
(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем)

___.___. 20___ р.

Керівник освітньої програми _____ В.Л. Бурячок
(підпис)

Робочу програму перевірено

___.___. 20___ р.

Заступник директора/декана _____ І.Ю. Мельник
(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	6 / 180	
Курс	5	
Семестр	10	
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	6	
Обсяг годин, в тому числі:	180	
Аудиторні	48	
Модульний контроль	10	
Семестровий контроль	30	
Самостійна робота	92	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Технології безпеки Web-ресурсів» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів другого (магістерського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої 125.00.02 «Безпека інформаційних і комунікаційних систем».

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Технології безпеки Web-ресурсів» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Технології безпеки Web-ресурсів» складається з трьох змістових модулів: «Впровадження методів захисту в протоколах обміну інформацією», «Веб-атаки (уразливості)», «Розробка захищених об'єктів. Проекти OWASP». Обсяг дисципліни – 180 год. (6 кредитів).

Метою викладання навчальної дисципліни «Технології безпеки Web-ресурсів» є формування у студентів уміння вирішувати задачі адміністрування апаратного і програмного забезпечення веб-ресурсів, застосовувати нормативно-правові, організаційні та технічні процедури при роботі веб-ресурсів.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері забезпечення безпеки веб-ресурсів, їх інформаційної та кібернетичної безпеки та набуття **наступних компетентностей**:

Фахова компетентність

КФ-3 — здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

3. **Результати навчання за дисципліною**

У результаті вивчення навчальної дисципліни студент повинен
знати:

- протоколи зв’язку;
- загальні навички програмування;
- веб-технології (PHP, Java тощо);
- архітектуру веб-ресурсів, мов і протоколів, що використовуються при їх розробці і роботі (PHP, SQL, HTML, HTTP, IP, TCP, UDP, IP, Java, JavaScript);
- стандарти безпеки веб-сервіси, різноманітність веб-уразливостей;
- протоколи та законодавство про конфіденційність та кібербезпеку.

уміти:

- застосовувати і закривати уразливості веб-додатків різних типів;
- запропоновувати заходи для усунення та мінімізації наслідків проникнення.

та досягти наступних **програмних результатів навчання:**

ПРз-6 — знати існуючі уразливості Web-ресурсів (SQL-ін’єкції, брутфорс, XSS й т. ін.) та способи боротьби з ними на етапі розробки та в процесі експлуатації; знати шаблони проектування безпечних Web-додатків.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Впровадження методів захисту в протоколах обміну інформацією							
Тема 1. Протоколи HTTP/S, SOAP	26	4		4	4		14
Тема 2. Захист конфіденційності клієнт-серверного додатку через протокол поштового відділення, простий протокол передачі пошти та протокол доступу до інтернет-повідомлень	20	2		2	2		14
Модульний контроль	2						
Разом	48	6		6	6		28
Змістовий модуль 2. Веб-атаки (уразливості)							
Тема 3. Веб-системи та архітектура веб-додатків	28	4		4	4		16
Тема 4. Аутентифікація та авторизація	22	2		2	2		16
Модульний контроль	2						
Разом	52	6		6	6		32
Змістовий модуль 3. Розробка захищених об’єктів. Проекти OWASP							
Тема 5. Методології розробки захищених об’єктів	22	2		2	2		16
	22	2		2	2		16

Тема 6. Вступ до проекту тестування

OWASP							
Модульний контроль	6						
Разом	50	4		4	4		32
Підготовка та проведення контрольних заходів	30						
Усього	180	16		16	16		92

5. Програма навчальної дисципліни

Змістовий модуль 1. Впровадження методів захисту в протоколах обміну інформацією

Основні питання:

- Протокол передачі гіпертексту.
- HTTP-запити та відповіді, методи та повідомлення.
- Кукі.
- HTTPS (протокол передачі гіпертексту через захищені сокети).
- Протокол SSL (Secure Sockets Layer).
- Симетричне та асиметричне шифрування.
- Перехоплення проксі та HTTPS.
- 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 (уразливості)

Основні питання:

- 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).
- Прогнозування вхідних даних/сеансів.
- Недостатня авторизація.
- Недостатнє закінчення сеансу.
- Фіксація сеансу.
- Викрадення сеансу.
- Перехресні сценарії (XSS).
- Сценарії крос-кадрів (XFS) або iframe-ін’єкція.
- Підробка запитів на місцях, CSRF.
- Зловживання JSON.
- Переповнення буфера.
- LDAP-ін’єкція.
- SQL-ін’єкція.
- SSI-ін’єкція.
- XPath-ін’єкція.
- Індексування каталогів.
- Витоки інформації.
- Пошук шляху (трасування).
- Передбачуване розташування ресурсів.

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

Основні питання:

- Забезпечення технологій веб-додатків (SWAT).
- Обробка помилок та ведення журналу.
- Аутентифікація.
- Обробка вхідних і вихідних даних.
- Конфігурація та операції.
- Управління сеансами.
- Контроль доступу.
- Про 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.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп'ютерного контролю:* програми-емулятори.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	3	3	3	3	2	2
Відвідування семінарських занять	1						
Відвідування практичних занять	1	3	3	3	3	2	2
Відвідування лабораторних занять	1	3	3	3	3	2	2
Робота на семінарському занятті	10						
Робота на практичному занятті	10	3	30	3	30	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	10	3	30	3	30	2	20
Виконання завдань для самостійної роботи	5	2	10	2	10	2	10
Виконання модульної роботи	25	1	25	1	25	1	25
Виконання ІНДЗ	30						
Разом		-	104	-	104	-	81
Максимальна кількість балів: 289							
Розрахунок коефіцієнта: 289/60=4,82							

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Впровадження методів захисту в протоколах обміну інформацією		28	10
1	Основи методи захисту в протоколах обміну інформацією: • виконання завдань відповідно до теми; • опрацювання фахових видань.	28	10
Змістовий модуль 2. Веб-атаки (уразливості)		32	10
2	Порядок проведення веб-атаки: • виконання завдань відповідно до теми; • опрацювання фахових видань.	32	10
Змістовий модуль 3. Розробка захищених об’єктів. Проекти OWASP		32	10
3	Методи використання функціоналу бібліотеки проекту OWASP: • виконання завдань відповідно до теми; • опрацювання фахових видань.	32	10
Разом		92	30

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення — тест, що складається 3 комплексних запитань.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Екзамен оцінюється у 40 балів за розподілом: 20 балів – комплексний комп'ютерний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь необхідних для побудови ІТ-інфраструктури освітнього закладу.

Бали за виконання тесту та бали за виконання практичного завдання додаються. Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

Підсумкова кількість балів (max – 40)	Оцінка за 4-бальною шкалою
1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

Орієнтовний перелік питань для семестрового контролю

1. Протокол передачі гіпертексту.
2. HTTP-запити та відповіді, методи та повідомлення.
3. Кукі.
4. HTTPS (протокол передачі гіпертексту через захищені сокети).
5. Протокол SSL (Secure Sockets Layer).
6. Симетричне та асиметричне шифрування.
7. Перехоплення проксі та HTTPS.

8. Використання протоколу простого доступу до об’єктів (SOAP).
9. Протокол SMTP (Simple Mail Transfer Protocol).
10. Протокол поштового відділення (POP3).
11. Протокол доступу до Інтернету (IMAP).
12. Архітектура веб-систем і веб-додатків.
13. Об’єкти захисту/атаки.
14. Класифікація веб-атак (уразливості).
15. Груба сила (Brute Force).
16. Недостатня аутентифікація.
17. Недостатнє відновлення пароля (перевірка слабкого відновлення пароля).
18. Прогнозування вхідних даних/сеансів.
19. Недостатня авторизація.
20. Недостатнє закінчення сеансу.
21. Фіксація сеансу.
22. Викрадення сеансу.
23. Перехресні сценарії (XSS).
24. Сценарії крос-кадрів (XFS) або iframe-ін’єкція.
25. Підробка запитів на місцях, CSRF.
26. Зловживання JSON.
27. Переповнення буфера.
28. LDAP-ін’єкція.
29. SQL-ін’єкція.
30. SSI-ін’єкція.
31. XPath-ін’єкція.
32. Індексування каталогів.
33. Витоки інформації.
34. Пошук шляху (трасування).
35. Передбачуване розташування ресурсів.
36. Забезпечення технологій веб-додатків (SWAT).
37. Обробка помилок та ведення журналу.
38. Аутентифікація.
39. Обробка вхідних і вихідних даних.
40. Конфігурація та операції.
41. Управління сеансами.
42. Контроль доступу.
43. Про проект тестування OWASP.
44. Принципи тестування.
45. Пояснення техніки тестування.
46. Виведення вимог до тестування безпеки.
47. Тести безпеки, інтегровані в робочі процеси розробки та тестування.
48. Аналіз і звітність тестових даних безпеки.
49. Інструменти тестування.
50. Основні поняття аудиту веб-додатків.
51. Методика організації та проведення аудиту веб-додатків.

Шкала відповідності оцінок

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	Значення оцінки
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре — достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре — в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно — посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо — мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання — незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу — досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 180 год., лекції – 16 год., практичні заняття – 16 год., лабораторні роботи – 16 год., модульний контроль – 10 год., семестровий контроль – 30 год., самостійна робота – 92 год.

Модулі (назви, бали)	**Змістовий модуль 1. Впровадження методів захисту в протоколах обміну інформацією (104 бали)**		**Змістовий модуль 2. Веб-атаки (уразливості) (104 бали)**		**Змістовий модуль 3. Розробка захищених об'єктів. Проекти OWASP (81 бали)**	
Лекції (теми, бали)	Протоколи HTTP/S, SOAP (2 бали)	Захист конфіденційності клієнт-серверного додатку через протокол поштового відділення, простий протокол передачі пошти та протокол доступу до інтернет-повідомлень (1 бал)	Веб-системи та архітектура веб-додатків (2 бали)	Аутентифікація та авторизація (1 бал)	Методології розробки захищених об'єктів (1 бал)	Вступ до проекту тестування OWASP (1 бал)
Практичні, семінарські заняття (теми, бали)	Протоколи HTTP/S (22 бали)	Безпека веб-додатків (11 балів)	Атаки на стороні клієнта (22 бали)	Розкриття інформації (11 балів)	Аудит безпеки веб-додатків (11 балів)	Наскрізні сценарії на основі DOM (11 балів)
Лабораторні заняття (теми, бали)	Цифровий SQL-ін'єкції (22 бали)	Загрози та вразливості веб-додатків (11 балів)	Збережена атака XSS (22 бали)	Підробка запиту на мульти-сайти (CSRF) (11 балів)	Фільтрація на стороні клієнта (11 балів)	DOM-ін'єкції (11 балів)
Самостійна робота	Самостійна робота (10 балів)		Самостійна робота (10 балів)		Самостійна робота (10 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 2 (25 балів)		Модульна контрольна робота 3 (25 балів)	
Підсумковий контроль (вид, бали)	Екзамен (40 балів)					

8. Рекомендовані джерела

Основна (базова):

1. Gerardus Blokdyk. OWASP: Third Edition, 2018.
2. Binkly Schiller. Botnets: The Killer Web App.
3. Andres Andre. Professional Pen Testing for Web Applications.

Додаткова

1. Michael Hartl, Aurelius Prochazka. RailsSpace: Building a Social Networking Website with Ruby on Rails.
2. Dafydd Stuttard, Marcus Pinto. The Web Application Hacker’s Handbook.

9. Додаткові ресурси

1. https://www.owasp.org/index.php/Category:OWASP_Books