Волинський національний університет імені Лесі Українки
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативної навчальної дисципліни

Безпека Web-ресурсів та додатків

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека
Форма навчання	Денна
Розробник (викладач)	Яцюк Світлана Миколаївна, кандидат педагогічних наук, доцент
Контактна інформація	Електронна адреса викладача: Yatsyuk.Svitlana@vnu.edu.ua Телефон: 050-76-16-380
Програма навчальної дисципліни	Програма навчальної дисципліни розміщена на сторінці кафедри комп'ютерних наук та кібербезпеки ВНУ імені Лесі Українки
Семестр, курс	7 семестр, 7 курс
Обсяг дисципліни	Загальний обсяг: 4 кредитів / 120 годин. Аудиторних годин: 54; з них: лекцій – 24 год., лабораторних – 30 год. Самостійної роботи: 58 години.
Форма контролю	Іспит (7 семестр)
Час занять	Тижневих годин: 7 семестр – 3 год Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Анотація дисципліни	Дана дисципліна вивчається один семестр. В процесі вивчення дисципліни розглядаються основи безпеки рівня веб-серверу, а саме особливості побудови та розгортання сучасного веб-сайту на базі системи управління вмістом (CMS), засоби безпеки рівня серверної інфраструктури, особливості застосування технології віртуалізації рівня операційної системи. При вивченні архітектури веб-систем та взаємодії між веб-сервісами, особлива увага звертається на об'єкти захисту/атаки, аутентифікацію та авторизацію, забезпечення безпеки даних. особливості застосування баз даних для побудови захищених веб-рішень, відкриті проекти по забезпеченню безпеки веб-додатків та перспективи організації та виконання тестування рівня безпеки для певного веб-ресурсу.
Предреквізити дисципліни	Інформаційні системи та інтернет-технології, введення в мережі, комплексні системи захисту інформації, вміння використовувати ОС Linux, знання особливостей побудови корпоративних мереж.
Постреквізити дисципліни	Безпосереднє застосування результатів навчання при вивченні курсів «Програмування скриптовими мовами», «Технологія програмування захищених систем», «Моделювання та безпека соціальних процесів», при написанні дипломних проектів щодо даної тематики, забезпечення комплексного захисту бізнес-процесів компанії чи підприємства на рівні веб-рішення.
Мета вивчення дисципліни	Формування у студентів уміння вирішувати задачі адміністрування апаратного і програмного забезпечення веб-ресурсів, застосовувати нормативно-правові, організаційні та технічні процедури при роботі

	веб-ресурсів. Загальні компетентності: ЗК2 Знання та розуміння предметної області та розуміння професії. ЗК4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. Фахові компетентності: СК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.
Результати навчання	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. (ПРН 23) Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. (ПРН 48) Вирішувати задачі аналізу програмного коду на наявність можливих загроз. (ПРН 53)

Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Усього	у тому числі			
		Лекції	Лабораторні заняття	Консультації	Самостійна робота
Змістовий модуль 1.					
Тема 1. Проблеми конфіденційності в Інтернеті.	12	2	2		8
Тема 2. Особливості побудови та розгортання сучасного веб-сайту на базі системи управління вмістом (CMS)	20	2	6	2	10
Тема 3. Засоби безпеки рівня серверної інфраструктури. Особливості застосування технології віртуалізації рівня операційної системи.	24	6	6	2	10
Тема 4. Архітектура веб-систем. Об'єкти захисту/атаки.	24	6	6	2	10
Тема 5. Взаємодія між веб-сервісами. REST-інтерфейс та його безпека.	22	4	6	2	10
Тема 6. Перспективи організації та виконання тестування рівня безпеки для певного веб-ресурсу	18	4	4		10
Разом за змістовим модулем 1	**120**	**24**	**30**	**8**	**58**

Оцінювання

Оцінювання навчальних досягнень здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання лабораторних робіт, самостійне розв'язання індивідуальних завдань) та підсумковий модульний контроль (тестова модульна контрольна робота). Максимальна кількість балів, яку може заробити студент під час поточного оцінювання за семестр – 40 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за модульну контрольну роботу (МКР). Максимальна кількість балів, яку може заробити студент під час модульного контролю за семестр складає 60 балів.

1 семестр

Поточний контроль (40 балів)			Модульний контроль (60 балів)	Загальна кількість балів
Модуль 1		Модуль 2	Модуль 3	
Змістовий модуль 1		ІНДЗ	МКР 1	
Т 1-4	Т 5-6	Т 1-7	Т 1-6	100
15	15	10	60	

Передбачається виконання індивідуальних завдань. Варіант ІНДЗ включає себе набір завдань, що охоплюють одну або кілька близьких тем. Письмові модульні контрольні роботи містять тестові завдання відповідного змістового модуля.

Якщо за результатами семестру накопичено не менше 75 балів і студент погоджується із цим результатом, то оцінка за семестр може виставлятися без складання заліку. В іншому разі студент складає залік; максимальна кількість балів, яку можна отримати на заліку – 60 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий контроль при цьому зберігається. Залік проходять у тестовій формі. Оцінка за семестр у випадку складання заліку є сумою балів поточного контролю та балів, отриманих під час заліку.

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загальноприйнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування. Очікується, що всі студенти відвідають усі лекції і лабораторні заняття курсу.

Політика щодо академічної доброчесності

Під час навчання учасники освітнього процесу зобов'язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання.

Політика щодо дедлайнів та перескладання

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи навчальні посібники, конспекти лекцій, виконують всі завдання для аудиторних занять, всі домашні завдання. Прозвітуватися про виконання завдань можна під час консультацій, одночасно при цьому з'ясувати незрозумілі моменти, задати запитання викладачу.

Перескладання модульних контрольних робіт заборонено. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.

Рекомендована література

1. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

2. Евсеев С. П. Концептуальная синергетическая модель оценки безопасности банковской безопасности в организациях банковского сектора / С. П. Евсеев, О. Г. Король // Матеріали Міжнародної науково-практичної конференції" Проблеми і перспективи розвитку ІТ-індустрії ": тези доповідей, 20–21 квітня 2017 р. – Х. : ХНЕУ ім. С. Кузнеця, 2017. – С. 51.

3. Алексієв В. О. Застосування GRID-технології у транспортному ВНЗ : навч.-метод. посіб. / В. О. Алексієв.– Х. : ХНАДУ, 2008. – 208 с.

4. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. – СПб.:

Питер, 2020. – 448 с.
5. Топ-10 OWASP -2017Десять самых критичных угроз безопасности веб-приложений. [Электронный ресурс] – Режим доступа : https://owasp.org/www-pdf-archive/OWASP_Top_10-2017-ru.pdf
6. Уильямс Б., Дэмстра Д., Стэрн Х. WordPress для профессионалов. – СПб.: Питер, 2014. – 464 с.
7. Holistic Info-Sec for Web Developers. [Electronic resource]. –Access mode: https://holisticinfosecforwebdevelopers.com/
OWASP Web Security Testing Guide. [Electronic resource]. –Access mode : https://owasp.org/www-project-web-security-testing-guide/

Силабус навчальної дисципліни, затверджено на засіданні кафедри

Комп'ютерних наук та кібербезпеки
протокол № 3 від 05.10.2020р.

Завідувач кафедри:  Сачук Ю.В.