МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
нормативного освітнього компонента
ЗАХИСТ ВЕБРЕСУРСІВ ТА ДОДАТКІВ
підготовки здобувачів освіти
першого (бакалаврського) рівня

спеціальності 125 Кібербезпека та захист інформації

освітньо-професійної програми

Кібербезпека та захист інформації

Луцьк – 2023

Силабус нормативного освітнього компонента «Захист вебресурсів та додатків**»** підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації.

Розробник:
Павленко Юлія Степанівна, старший викладач кафедри комп'ютерних наук та кібербезпеки

Погоджено
Гарант освітньо-професійної програми:  Глинчук Л.Я.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки
протокол № 2 від 28 вересня 2023 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна /освітньо-наукова/освітньо-творча програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="8">12 Інформаційні технології,
125 Кібербезпека та захист інформації,
Кібербезпека та захист інформації, бакалавр</td><td>Нормативна</td></tr>
<tr><td>Рік навчання 3</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 120 / 4</td><td>Семестр 6-ий</td></tr>
<tr><td>Лекції 30 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Лабораторні 36 год.</td></tr>
<tr><td>Самостійна робота 46 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td colspan="2">Мова навчання</td><td>Форма контролю: екзамен
українська</td></tr>
</table>

ІІ. Інформація про викладача (-ів)

ПІП Павленко Юлія Степанівна
Посада старший викладач кафедри комп’ютерних наук та кібербезпеки
Контактна інформація: Pavlenko.Yulya@vnu.edu.ua.
Дні занять: http://194.44.187.20/cgi-bin/timetable.cgi?n=700.

ІІІ. Опис освітнього компонента

Анотація курсу. Освітній компонент «Захист вебресурсів та додатків» є нормативним та належить до циклу професійної підготовки освітнього ступеня бакалавр спеціальності 125 Кібербезпека та захист інформації, забезпечує професійний розвиток бакалавра та спрямована на формування у майбутніх фахівців базових знань, вмінь та навичок у сфері захисту вебресурсів та особливостей проектування додатків з врахуванням можливих загроз.

Мета і завдання освітнього компонента. вивчення технологій, засобів та методів проведення атак на вебдодатки, виявлення вразливостей та усунення їх наслідків; оволодіння знаннями та навичками щодо діагностування вразливостей вебдодатків та аналізу програмного коду на наявність можливих загроз.

Результати навчання (Компетентності).

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
ЗК 2. Знання та розуміння предметної області та розуміння професії.
ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою.
ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

1. **Структура освітнього компонента.**

Назви змістових модулів і тем	**Усього**	**Лек.**	**Лабор.**	**Сам. роб.**	**Конс.**	**Форма контролю/ Бали**
Тема 1. Огляд архітектурних підходів до проєктування вебдодатків.	4	2		2		
Тема 2. Класифікація вразливостей вебресурсів та атак на них.	4	2		2		
Тема 3. Вимоги до захисту інформації вебсторінки від несанкціонованого доступу. Нормативно-правова база	10	4	2	4		звіт / 2 Т / 10
Тема 4. Міжсайтовий скриптинг (XSS) та засоби захисту від нього.	11	2	4	4	1	звіт / 4
Тема 5. SQL-ін'єкції та засоби захисту. Атака на клієнта: підробка міжсайтових запитів (CSRF / XSRF).	11	2	4	4	1	звіт / 4 Т / 10
Тема 6. Злом аутентифікації та сеансу. Clickjacking.	9	2	2	4	1	звіт / 4
Тема 7. Міжсайтові запити CSRF.	11	2	4	4	1	звіт / 4
Тема 8. Cookie атаки з перехоплення інформації.	11	2	4	4	1	звіт / 4 Т / 10
Тема 9. Інструменти тестування уразливостей вебресурсів.	6	2	2	2		звіт / 3
Тема 10. XXE (XML eXternal Entity)-атаки. DDoS-атаки.	11	2	4	4	1	звіт / 4 Т / 10
Тема 11. Міжмережеві екрани. Міжмережеві екрани для вебресурсів.	9	2	2	4	1	звіт / 2
Тема 12. Використання інструментів захисту вебресурсів	11	2	4	4	1	звіт / 4
Тема 13. Підходи до тестування вебресурсів.	6	2	2	2		звіт / 3
Тема 14. Загальна характеристика методологій тестування безпеки:	6	2	2	2		звіт / 2 Т / 20

OSSTMM, PTES, OWASP Testing Guide.						
Всього годин/Балів	120	30	36	46	8	100

Методи контролю*: ДС – дискусія, ДБ – дебати, Т – тести, ТР – тренінг, РЗ/К – розв'язування задач/кейсів, ІНДЗ/ІРС – індивідуальне завдання/індивідуальна робота здобувача освіти, РМГ – робота в малих групах, МКР/КР – модульна контрольна робота/ контрольна робота, Р – реферат, а також аналітична записка, аналітичне есе, аналіз твору тощо.

2. Завдання для самостійного опрацювання.

№ з/п	Тема	Кількість годин
1	Опрацювання лекційного матеріалу	8
2	Підготовка до лабораторних робіт	18
3	Підготовка до тестового контролю	10
4	Підготовка до іспиту	10
	Разом	46

IV. Політика оцінювання

Політика щодо відвідування занять. Для здобувачів вищої освіти денної форми відвідування заняття є обов'язковим. Поважними причинами для неявки на заняття є хвороба, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту. За об'єктивних причин навчання може відбуватись в онлайн формі за погодженням з завідувачем кафедрою та деканом факультету.

Політика щодо академічної доброчесності. Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання ОК і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). У разі порушення здобувачем вищої освіти академічної доброчесності робота оцінюється незадовільно та має бути виконана повторно, а результати раніше зданих робіт анулюються і виконуються повторно у порядку, визначеному викладачем. При цьому викладач залишає за собою право змінити 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, матеріали електронного курсу «Захист вебресурсів та додатків», розміщеного на платформі дистанційного навчання Moodle кафедри комп'ютерних наук та кібербезпеки, виконують всі завдання.

Прозвітуватися про виконання завдань можна, використовуючи електронний курс «Захист вебресурсів та додатків», розміщений на платформі дистанційного навчання Moodle кафедри комп'ютерних наук та кібербезпеки, або під час консультацій. Існує можливість використання форуму електронного курсу. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.

Терміни здачі робіт зазначені в електронному курсі навчальної дисципліни. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).

Політика щодо оскарження оцінювання. Якщо здобувач вищої освіти не згоден з оцінюванням його знань, він може опротестувати виставлену викладачем оцінку у встановленому порядку. Проте, якщо опротестування безпідставне, можливе зменшення оцінки.

Політика щодо визнання результатів, отриманих у формальній, неформальній та/або інформальній освіті. Під час вивчення освітнього компонента можливе визнання результатів навчання отриманих у формальній, неформальній та/або інформальній освіті. Порядок визнання результатів навчання для здобувачів вищої освіти, набутих у: формальній освіті (академічна мобільність студентів на території України чи поза її межами, для студентів, які переводяться, поновлюються з інших ЗВО (вітчизняних чи іноземних); неформальній та/або інформальній освіті здійснюється згідно «ПОЛОЖЕННЯ про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки».

V. Підсумковий контроль

Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе поточний контроль (нараховується за якісне виконання лабораторних робіт) та підсумковий модульний контроль. Максимальна кількість балів, яку може отримати студент під час поточного оцінювання за семестр – 40 балів. Підсумковий контроль за семестр включає в себе оцінки за тестування та складає 60 балів.

Якщо за результатами семестру здобувачем освіти накопичено не менше 75 балів і він погоджується із цим результатом, то оцінка за семестр може виставлятися без складання заліку. В іншому випадку здобувач освіти складає іспит; максимальна кількість балів, яку можна отримати на іспиті – 60 балів, при цьому бали за підсумковий модульний контроль анульовуються.

Іспит проходить у письмовій формі.

Перелік питань до іспиту.

Поняття архітектури проєктування вебдодатків.
Характеристика монолітної архітектури.
Характеристика мікросервісів.
Характеристика безсерверної архітектури.
Класифікація вразливостей вебресурсів та атак на них.
Вимоги до захисту інформації вебсторінки від несанкціонованого доступу.
Нормативно-правова база
Поняття міжсайтового скриптинг (XSS).
Засоби захисту від XSS.
Поняття SQL-ін’єкції.
Засоби захисту від SQL-ін’єкції..
Атака на клієнта: підробка міжсайтових запитів (CSRF / XSRF).
Злом аутентифікації та сеансу. Clickjacking.
Міжсайтові запити CSRF.
Cookie атаки з перехоплення інформації.
Інструменти тестування уразливостей вебресурсів.
XXE (XML eXternal Entity)-атаки.
DDoS-атаки.

Поняття міжмережевого екрану.
Міжмережеві екрани для вебресурсів.
Використання інструментів захисту вебресурсів
Підходи до тестування вебресурсів.
Загальна характеристика методологій тестування безпеки: OSSTMM, PTES, OWASP Testing Guide.

VI. Шкала оцінювання

Оцінка в балах	Лінгвістична оцінка	Оцінка за шкалою ECTS	
		оцінка	пояснення
90–100	Відмінно	A	відмінне виконання
82–89	Дуже добре	B	вище середнього рівня
75–81	Добре	C	загалом хороша робота
67–74	Задовільно	D	непогано
60–66	Достатньо	E	виконання відповідає мінімальним критеріям
1–59	Незадовільно	Fx	Необхідне перескладання

VI. Рекомендована література та інтернет-ресурси.

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. Веб-портал Державної служби технічного захисту інформації України». – URL : www.dstszi.gov.ua.
3. Веб-портал системи виявлення вразливостей Snort. – Режим доступу : www.snort.com
4. Kimminich B. Pwining OWASP Juice Shop. 2020. – 301 p.
5. Andrew Hoffman. Web Application Security. Published by O'Reilly Media, Inc. 2020. – 331 p.
6. ITU-T Rec. X.805. Security architecture for systems providing end-to-end communications. [Електронний ресурс] / ITU-T Recommendation X.805, 10/2003. URL : https://www.itu.int/rec/T-REC-X.805-200310-I/en.
7. 12 NIST Special Publication 800-33. Underlying Technical Models for Information Technology Security. [Електронний ресурс] / Gary Stoneburner. CODEN: NSPUE2, December 2001. URL : http://csrc.nist.gov/publications/nistpubs/800- 33/sp800-33.pdf.
8. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements.
9. Application Security Verification Standard 4:.0 – URL: https://www.owasp.org/images/d/d4/OWASP_Application_Security_Verification_Standard_4.0-en.pdf.
10. MITRE Common Weakness Enumeration – URL : https://cwe.mitre.org/.

11. National Institute of Standards and Technology – URL : https://nvd.nist.gov/vuln-metrics/cvss .
12. Open Web Application Security Project – URL : https://www.owasp.org/index.php/Category: OWASP_Code_Review_Project Holistic Info-Sec for Web Developers.
13. OWASP Web Security Testing Guide. [Electronic resource]. – URL : https://owasp.org/www-project-web-security-testing-guide/
14. Positive Technologies. What is a cross-site scripting (XSS) attack?. Positive Technologies - vulnerability assessment, compliance management and threat analysis solutions. URL: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/what-is-a-cross-site-scripting-xss-attack/
15. Підручник із інструменту тестування доступності WAVE - Засоби Тестування Програмного Забезпечення. URL : https://uk.myservername.com/wave-accessibility-testing-tool-tutorial