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

БЕЗПЕКА ВЕБ-РЕСУРСІВ ТА ДОДАТКІВ

підготовки бакалавра

спеціальності 125 Кібербезпека

освітньо-професійної програми
Інформаційна безпека

Луцьк – 2021

Силабус навчальної дисципліни «Безпека Веб-ресурсів та додатків**»** підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека, за освітньою програмою Інформаційна безпека.

Розробник: Яцюк С. М, доцент кафедри комп'ютерних наук та кібербезпеки, кандидат педагогічних наук.

Погоджено
Гарант освітньо-професійної програми:

Глинчук Л.Я.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 2 від 29 вересня 2022 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітньо-професійна /освітньо-наукова/освітньо-творча програма, освітній рівень</td><td>Характеристика освітнього компонента</td></tr>
<tr><td>Денна форма навчання</td><td rowspan="8">12 Інформаційні технології

125 Кібербезпека

Інформаційна безпека</td><td>Нормативний</td></tr>
<tr><td rowspan="4">Кількість годин/кредитів 120/4</td><td>Рік навчання: 3</td></tr>
<tr><td>Семестр: 5</td></tr>
<tr><td>Лекції: 24 год.</td></tr>
<tr><td>Лабораторні роботи: 34год.</td></tr>
<tr><td rowspan="4">ІНДЗ: немає</td><td>Самостійна робота: 54 год.</td></tr>
<tr><td>Консультації: 8 год.</td></tr>
<tr><td>Форма контролю: екзамен</td></tr>
<tr><td colspan="2">Мова навчання</td><td>Українська</td></tr>
</table>

ІІ. Інформація про викладача

ПІП **Яцюк Світлана Миколаївна**
Науковий ступінь **кандидат педагогічних наук**
Вчене звання - **доцент кафедри комп'ютерних наук та кібербезпеки**
Посада **доцент кафедри комп'ютерних наук та кібербезпеки**
Контактна інформація Yatsyuk.Svitlana@eenu.edu.ua
Дні занять **http://194.44.187.20/cgi-bin/timetable.cgi?n=700**

ІІІ. Опис дисципліни

1. **Анотація ОК.** 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 баз 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 1.перспективи організації та виконання тестування рівня безпеки для певного веб-ресурсу.
2. **Предреквізити ОК.** Інформаційні системи та інтернет-технології, введення в мережі, вміння використовувати ОС Linux, знання особливостей побудови корпоративних мереж.
3. **Постреквізити ОК.** Безпосереднє застосування результатів навчання при вивченні курсів «Програмування скрипковими 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.
4. **Мета і завдання навчальної дисципліни.**
   Метою ОК є формування теоретичних знань та практичних умінь у сфері забезпечення безпеки веб-ресурсів, їх інформаційної та кібернетичної безпеки. Забезпечення комплексного захисту бізнес-процесів компанії чи підприємства на рівні вебрішення. Розглядаються основи програмування захищених веб-сайтів та засоби серверної безпеки рівня веб-серверу, бази даних, засобів авторизації та аутентифікації користувачів.

IV. Результати навчання (Компетентності) відповідно до освітньо-професійної програми 2021 р.

Знання	Вміння
ЗК 2. Знання та розуміння предметної області та розуміння професії.	ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та кібербезпеки.
ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
	ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних автоматизованих) систем згідно встановленої політики інформаційної та кібербезпеки.
	ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної такібербезпеки.
Компетенції відповідно до вимог роботодавців	
1. Знати міжнародні та державні стандарти по забезпеченню безпеки Web-ресурсів.	1. Проводити оцінку наявності уразливостей та пошук уразливостей у Web-додатках (SQL-ін'єкції, XSS, CSRF, buffer overflow, тощо).
2. Знати існуючі Web-загрози відповідно до міжнародних та державних стандартів по забезпеченню безпеки Web-ресурсів.	2. Проводити аудит процесів інформаційної безпекищодо захисту Web-ресурсів від сучасних загроз.
3. Знати основи методів адміністрування сучасних інструментів дослідження уразливостей Web-ресурсів.	3. Проводити моніторинг та контроль вторгнень за допомогою інструментів тестування з розширеними функціями і сучасними інфраструктурами.
Результати навчання відповідно до ОПП	
1. ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку якості прийнятих рішень.	
2. ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	
3. ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	
4. ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	
5. ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).	
6. ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.	

V. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Усього	у тому числі				
		Лекції	Лабораторні заняття	Консультації	Самостійна робота	Форма контролю/ Бали
Змістовий модуль 1. Основи безпеки рівня веб-серверу.						
Тема 1. Введення. Основні терміни та визначення.	7			1	6	Усне опитув./ 2
Тема 2. Особливості побудови та розгортання сучасного веб-сайту на базі системи управління вмістом (CMS).	16	4	4	1	7	Лаб.роб. /2
Тема 3. Засоби безпеки рівня серверної інфраструктури. Особливості застосування технології віртуалізації рівня операційної системи.	18	4	6	1	7	Лаб.роб. /4
Тема 4. Архітектура веб-систем. Об'єкти захисту/атаки. Аутентифікація та авторизація	16	4	4	1	7	Лаб.роб. /3
Тема 5. Взаємодія між веб-сервісами. REST-інтерфейс та його безпека.	16	4	4	1	7	Лаб.роб. /3
Разом за змістовим модулем 1	**73**	**16**	**18**	**5**	**34**	**14 балів**
Змістовий модуль 2. Практика забезпечення безпеки веб-ресурсів						
Тема 6. Забезпечення безпеки даних. Особливості застосування баз даних для побудови захищених веб-рішень	23	4	6	1	12	Лаб.роб. /5
Тема 7. Відкритий проект по забезпеченню безпеки веб-додатків (OWASP).	13	2	6	1	4	Лаб.роб. /5
Тема 8. Перспективи організації та виконання тестування рівня безпеки для певного вебресурсу.	11	2	4	1	4	Робота над проектом /6
Разом за змістовим модулем 2	**47**		**16**	**3**	**20**	**16 балів**
Разом	**120**	**24**	**34**	**8**	**54**	
Види підсумкових робіт						**Бал**
Модульна контрольна робота						**30**
ІНДЗ						**10**
Самостійна робота*						**30**
Всього						**100 балів**

Самостійна робота ЗО* виставляється за наявності сертифікатів з онлайн-курсів поданих на самостійне опрацювання (8, 7, 7, 4, 4 балів відповідно за курс)

6. Завдання для самостійного опрацювання

№	Тема
1.	Онлайн-курс «Інформаційна безпека» платформа https://prometheus.org.ua/
2.	Онлайн-курс «Інформаційна гігієна під час війни» платформа https://prometheus.org.ua/
3.	Онлайн-курс «Захист персональних даних» платформа https://www.ed-era.com/courses/
4.	Онлайн-курс «Основи кібергігієни» платформа https://osvita.diia.gov.ua/courses/
5.	Онлайн-курс «Безпека дітей в інтернеті» платформа https://osvita.diia.gov.ua/courses/
6.	Опрацювання лекційного матеріалу
7.	Виконання лабораторних робіт

7. Індивідуальне завдання у вигляді розрахунково-графічної роботи

Варіант 1. Настроїти систему захисту операційної системи.
Варіант 2. Розробити додаткові компонентів захисту операційної системи.
Варіант 3. Настроїти систему захисту електронної пошти від спаму.
Варіант 4. Розробити систему захисту електронної пошти від спаму. Варіант 5. Настроїти мережевий екран.
Варіант 6. Розробити додаткові компонентів захисту мережевих екранів.
Варіант 7. Дослідити систему розповсюдження спаму, з метою виявлення їх вразливостей.
Варіант 8. Дослідити мережеві сканери та розробити відповідну систему захисту.
Варіант 9. Дослідити Dos та Ddos атаки та розробити систему захисту від них.
Варіант 10. Дослідити особливості програмного забезпечення мобільних пристроїв.
Варіант 11. Настроїти систему захисту СУБД.
Варіант 12. Розробити додаткові компоненти захисту СУБД.
Варіант 13. Розробити засоби захисту СУБД від SQL ін'єкцій.
Варіант 14. Настроїти антивірусні засоби.
Варіант 15. Розробити систему антивірусного захисту.
Варіант 16. Настроїти систему захисту від кейлогерів.
Варіант 17. Розробити компонент захисту від кейлогерів.
Варіант 18. Настроїти захист віртуальної мережі.
Варіант 19. Дослідити засоби зламу парольного захисту операційних систем та розробити відповідну систему захисту.
Варіант 20. Розробити систему захисту офісних документів від несанкціонованого копіювання.
Варіант 21. Настроїти систему захисту програм та даних від несанкціонованого розповсюдження.
Варіант 22. Настроїти систему резервного копіювання інформації операційної системи.
Варіант 23. Дослідити стійкість віртуальної машини Java від атаки на відмову в обслуговуванні.
Варіант 24. Дослідити стійкість Framework від атаки на відмову в обслуговуванні.
Варіант 25. Настроїти систему безпеки веб-серверів.
Варіант 26. Розробити додаткові модулі захисту веб-серверів.
Варіант 27. Дослідити засоби зламу захисту програм з метою розробки відповідних систем захисту.
Варіант 28. Розробити систему захисту програм від вивчення.
Варіант 29. Настроїти систему виявлення вторгнень.
Варіант 30. Настроїти систему виявлення вразливостей. Варіант
31. Розробити систему виявлення вторгнень.
Варіант 32. Розробити систему виявлення вразливостей.
Варіант 33. Дослідити вразливості програмного забезпечення мобільних пристроїв з метою розробки системи їхнього захисту.

8. Політика курсу

Політика щодо оцінювання

Оцінювання знань здобувачів освіти здійснюється згідно **Положення про поточне та підсумкове оцінювання знань здобувачів освіти Волинського національного університету імені Лесі Українки**. Освітній компонент складається з двох змістових модулів та йоговивчення передбачає виконання лабораторних робіт. У цьому випадку підсумкова оцінка за 100-бальою шкалою складається із сумарної кількості балів за:
- поточне оцінювання з відповідних тем (максимум 40 балів);
- модульні контрольні роботи (максимум 60 балів).

Якщо за результатами семестру накопичено не менше 75 балів і здобувач освіти погоджується із цим результатом, то оцінка за семестр може виставлятися без складання екзамену. В іншому разі здобувач освіти складає екзамен; максимальна кількість балів, яку можна отримати на екзамені – 60 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий контроль при цьому зберігається. Оцінка за семестр у випадку складання екзамену є сумою балів поточного контролю та балів, отриманих під час екзамену. Повторне складання екзамену допускається не більше як два рази: один раз – викладачеві, другий – комісії, яку створює декан факультету.
Здобувачу освіти також можуть бути зараховані результати навчання, здобуті у процесі формальної, неформальної та/або інформальної освіти відповідно до «Положення про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки». Визнанню можуть підлягати результати навчання, що відповідають тематиці освітнього компоненту, його окремому розділу, темі (темам) або індивідуальному завданню, які здобувач освіти самостійно набув, вивчаючи освітні ресурси (семінари, інтернет-курси, професійні стажування та ін.) на онлайн-платформах Prometheus (https://prometheus.org.ua), EdEra (https://www.ed-era.com) та інших, і підтвердив відповідними сертифікатами.

Питання до екзамену

9. Види мереж і особливості їх функціонування.
10. Web-ресурси. WAN. LAN. WWW. Базові поняття.
11. Нормативна база щодо забезпечення захисту Webресурсів.
12. Основні поняття щодо безпеки Web -ресурсів .
13. Уразливості та загрози Web -ресурсів.
14. Технології виявлення уразливостей Web -ресурсів.
15. Уразливості та загрози Web -ресурсів.
16. Класифікація уразливостей
17. Класифікація сучасних attacks на Web -додатки.
18. Перелік засобів ЗІ Web - сторінок відповідно до вітчизняної нормативної бази .
19. Вимоги щодо захисту інформації Web -ресурсів.
20. Визначення основних уразливостей Web -систем на базі client -server.
21. Технології HTTP, SSL/TLS .
22. Безпека рівня мережевої інфраструктури ОІД.
23. Захист Web -додатків і сучасні напрями розвитку інформаційної та кібербезпеки.
24. Основні уразливості мережевих Web -додатків та методи їх усунення.
25. Сучасні методи тестування Web -ресурсів.
26. Security vulnerability testing для Web services.
27. Базові функції та напрями реалізації AppScan Standart.
28. Основні підходи та принципи роботи.
29. Black-box scanning, whitebox scanning, glass box scanning.
30. Принципи роботи, функції та можливості Vulnerability Scanner Software (VSS).
31. Особливості тестування, сучасні підходи до VSS.
32. Принципи застосування WASS, WAVS system.

33. Функціональні можливості. Механізми захисту Web-ресурсів.
34. Атаки на Webсистеми та методи протидії.
35. Метод тестування на проникнення.
36. Природа SQL injection та методи протидії. Переваги та недоліки методів.
37. Засоби сканування Web-сервісів.

Вирішення конфліктних ситуацій

Будь-яка конфліктна ситуація, яка виникає в учасників освітнього процесу вирішується згідно Положення про порядок і процедури вирішення конфліктних ситуацій у ВНУ імені Лесі Українки.

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально- прийнятих 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.

Методичне забезпечення ОК

1. Яцюк С. М. Безпека Web-ресурсів та додатків : курс лекцій. / С. М. Яцюк. – Луцьк : ПП Іванюк, 2020. 51 с.
2. Яцюк С. М. Веб-аналітика та пошукова оптимізація: Методичні рекомендації з дисципліни. Курс лекцій. / С. М. Яцюк. – Луцьк : ПП Іванюк, 2020. 50 с.

3. Яцюк С. М. Web-дизайн. Безпека Web-ресурсів та додатків: навчальний посібник./ С. М. Яцюк, В. Л. Юнчик. – Луцьк: ПП Іванюк, 2021. 316 с.
4. Яцюк С.М., Хомяк М.Я., Юнчик В.Л., Чепрасова Т.І. Особливості навчання веб-технологій розробки навчальних систем майбутніх вчителів інформатики та методика створення на їх основі власних освітніх ресурсів / Молодь і ринок. – 2021. № 7/193. С.118-122.
5. Яцюк С.М. Дистанційний курс Moodle: Безпека Web-ресурсів та додатків. Режим доступу: https://moodle.vnu.edu.ua/course/view.php?id=900.
6. Яцюк С. М., Пасічник В. В., Юнчик Л. В. Безпека інфраструктури комп'ютерних мереж : курс лекцій. – Луцьк : ПП Іванюк, 2020 р. – 90 с.

Рекомендована література

7. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко/ – К. : ДУТ – КНУ, 2016. – 178 с.
8. Яворський П. Основи веб-хакінгу. Пер. с англ. Бурмакін Е., 2016. – 201 с.
9. Яцюк С. М., Пасічник В. В., Юнчик Л. В. Безпека інфраструктури комп'ютерних мереж : курс лекцій. – Луцьк : ПП Іванюк, 2020 р. – 90 с
10. 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.
11. Веб-портал Державної служби технічного захисту інформації України». – Режим доступу : www.dstszi.gov.ua.
12. Веб-портал Державної служби технічного захисту інформації України». – Режим доступу : www.dstszi.gov.ua.
13. Веб-портал системи виявлення вразливостей Snort. – Режим доступу : www.snort.com
14. Kimminich B. Pwining OWASP Juice Shop. 2020. – 301 p.
15. Andrew Hoffman. Web Application Security. Published by O'Reilly Media, Inc. 2020. – 331 p.
16. ITU-T Rec. X.805. Security architecture for systems providing end-to-end communications. [Електронний ресурс] / ITU-T Recommendation X.805, 10/2003. Режим доступу: https://www.itu.int/rec/T-REC-X.805-200310-I/en.
17. 12 NIST Special Publication 800-33. Underlying Technical Models for Information Technology Security. [Електронний ресурс] / Gary Stoneburner. CODEN: NSPUE2, December 2001. Режим доступу: http://csrc.nist.gov/publications/nistpubs/800- 33/sp800-33.pdf.
18. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements.
19. Application Security Verification Standard 4:.0 https://www.owasp.org/images/d/d4/OWASP_Application_Security_Verification_Standard_4.0-en.pdf.
20. MITRE Common Weakness Enumeration: https://cwe.mitre.org/.
21. National Institute of Standards and Technology: https://nvd.nist.gov/vuln-metrics/cvss .
22. Open Web Application Security Project: https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project