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
ТЕХНОЛОГІЇ ВЕБРОЗРОБКИ ТА ЗАХИСТ ВЕБРЕСУРСІВ
підготовки здобувачів освіти першого (бакалаврського) рівня

спеціальності 125 Кібербезпека та захист інформації

освітньо-професійної програми

Кібербезпека та захист інформації

Луцьк – 2025

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

Розробники:
Юнчик Валентина Леонідівна, PhD, доцент кафедри комп'ютерних наук та кібербезпеки
Світницька Ірина Сергіївна, старший викладач кафедри комп'ютерних наук та кібербезпеки

Погоджено

Гарант освітньо-професійноїпрограми: Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки
протокол № 2 від 17.09.2025 р.

Завідувач кафедри: Гришанович Т. О.

І. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна 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 28 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Лабораторні 36 год.</td></tr>
<tr><td>Самостійна робота 48 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td colspan="2">Мова навчання</td><td>українська</td></tr>
</table>

ІІ. Інформація про викладачів

ПІП Юнчик Валентина Леонідівна
Науковий ступінь доктор філософії
Доцент кафедри комп’ютерних наук та кібербезпеки
Контактна інформація: Yunchyk.Valentyna@vnu.edu.ua
Дні занять: https://ps.vnu.edu.ua/cgi-bin/timetable.cgi

ПІП Світницька Ірина Сергіївна
Посада старший викладач кафедри комп’ютерних наук та кібербезпеки
Контактна інформація: *Svitnytska.Irina@vnu.edu.ua*
Дні занять *https://ps.vnu.edu.ua/cgi-bin/timetable.cgi*.

ІІІ. Опис освітнього компонента

1. Анотація ОК.

Освітній компонент «Технології веброзробки та захист вебресурсів» є нормативним та належить до циклу професійної підготовки освітнього ступеня бакалавр спеціальності 125 Кібербезпека та захист інформації, передбачає ознайомлення здобувачів вищої освіти із технологіями веброзробки, що використовуються під час програмування сучасних вебзастосунків. Розглядаються верстка вебсторінок з допомогою HTML та CSS, синтаксис, типи даних, структури даних, робота з формами, особливості обидвох мов, робота з DOM у JavaScript, робота з сесіями, cookies та базами даних в PHP, а також забезпечується формування у майбутніх фахівців базових знань, вмінь та навичок у сфері захисту вебресурсів та особливостей проектування додатків з врахуванням можливих загроз.

2. Пререквізити та постреквізити.

Пререквізити. Базові знання з інформаційних технологій та алгоритмізації, знання, вміння і навички, сформовані у ході вивчення ОК: «Бази данних»

Постреквізити. Освоєння даного освітнього компонента формує знання та вміння необхідні для подальшого проходження виробничої практики.

3. Мета і завдання освітнього компонента.

Сформувати у здобувачів вищої освіти компетентності із програмування вебзастосунків з допомогою мов програмування JavaScript та PHP та забезпечити 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.

1. Компетентності. Програмні результати навчання. Soft skills.

Інтегральна компетентність (ІК)

Здатність проектувати, розробляти та підтримувати веб-орієнтовані інформаційні системи на основі сучасних технологій клієнт-серверної архітектури, застосовуючи стандарти веб-програмування, принципи безпеки та інженерії програмного забезпечення, з використанням інструментів командної роботи та засобів контролю версій для розв’язання практичних та професійних задач у сфері ІТ.

Загальні компетентності (ЗК)

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 6. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.

ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності (СК)

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК 4. Здатність забезпечувати захист інформації інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання (РН)

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН 3. Застосовувати принципи неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

4. Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. Основи створення вебсторінок з допомогою HTML5 та CSS3 . Програмування на JS						**Т / 10**
Тема 1. Поняття та принципи роботи Інтернет. Протокол HTTP. Мова гіпертекстової розмітки HTML. Базові конструкції та синтаксис мови HTML.	6	2	2	2		Звіт по лаб. роботі / 5
Тема 2. Використання каскадних таблиць стилів CSS. Поняття CSS, селектора. Використання класів та ідентифікаторів. Наслідування та каскадування. Блочна структура вебсторінки.	9	2	2	4	1	Звіт по лаб. роботі / 5

Тема 3. JavaScript: призначення та можливості. Основи скриптової мови програмування JavaScript: типи даних та конструкції, мови масиви та об'єкти. Обробка даних форми.	8	2	2	4		Звіт по лаб. роботі / 5
Тема 4. Поняття DOM-структури документа. Навігація в DOM. Методи створення вузлів. Події в JavaScript.	11	2	4	4	1	Звіт по лаб. роботі / 5
Разом за модулем 1	34	8	10	14	2	20
Змістовий модуль 2. Програмування на PHP						**Т / 10**
Тема 5. PHP: призначення та можливості. Поняття клієнт-серверної архітектури вебдодатку. Локальний сервер. Основи мови програмування PHP: синтаксис, типи даних, змінні та константи, вирази, оператори.	6	2	2	2		Звіт по лаб. роботі / 5
Тема 6. PHP: керуючі конструкції, функції, робота з масивами та рядками. Робота з файлами в PHP. Обробка даних форм в PHP. HTTP-запити. Параметри URL.	11	2	4	4	1	Звіт по лаб. роботі / 5
Тема 7. Сесії та cookies	6	2	2	2		Звіт по лаб. роботі / 5
Тема 8. Робота з базою даних. MySQL	9	2	4	2	1	Звіт по лаб. роботі / 5
Тема 9. Фреймворк Laravel. Створення додатків на Laravel	9	2	2	4	1	Звіт по лаб. роботі / 5
Разом за модулем 2	41	10	14	14	3	25
Змістовий модуль 3. Захист вебресурсів						**Т / 10**
Тема 10. Класифікація вразливостей вебресурсів та атак на них. Вимоги до захисту інформації вебсторінки від несанкціонованого доступу. Нормативно-правова база.	8	2	2	4		Звіт по лаб. роботі / 5
Тема 11. Міжсайтовий скриптинг (XSS) та засоби захисту від нього. SQL-ін'єкції та засоби захисту. Атака на клієнта: підробка міжсайтових запитів (CSRF / XSRF).	9	2	2	4	1	Звіт по лаб. роботі / 5
Тема 12. Злом аутентифікації та сеансу. Clickjacking. Міжсайтові запити CSRF. Cookie атаки з перехоплення інформації.	11	2	4	4	1	Звіт по лаб. роботі / 5
Тема 13. Інструменти тестування уразливостей вебресурсів. XXE (XML eXternal Entity) - атаки. DDoS-атаки. Міжмережеві екрани для вебресурсів	8	2	2	4		Звіт по лаб. роботі / 5
Тема 14. Використання інструментів захисту вебресурсів. Загальна характеристика методологій тестування безпеки: OSSTMM, PTES, OWASP Testing Guide.	9	2	2	4	1	Звіт по лаб. роботі / 5
Разом за модулем 3	45	10	12	20	3	25
Всього годин/Балів	**120**	**28**	**36**	**48**	**8**	**100**

Методи контролю*: ЛР – лабораторна робота, Т – тести, РЗ/К – розв'язування задач/кейсів, ІНДЗ/ІР – індивідуальне завдання/індивідуальна робота здобувача освіти, МКР/КР – модульна контрольна робота/ контрольна робота.

5. Завдання для самостійного опрацювання.

№ з/п	Тема	Кількість годин
1	Підготовка до лабораторних робіт	30
2	Підготовка до тестового модульного контролю	8
3	Підготовка до іспиту	10
	Разом	48

IV. Політика оцінювання

Політика викладача щодо здобувача освіти. 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 та списування. Очікується, що всі здобувачі освіти відвідають усі лекції і лабораторні заняття освітнього компонента.

Політика щодо академічної доброчесності

Політика, стандарти та процедури дотримання академічної доброчесності у Волинському національному університеті імені Лесі Українки знайшли своє відображення в «Кодексі академічної доброчесності Волинського національного університету імені Лесі Українки». Вимоги до академічної доброчесності визначаються «Положенням про систему запобігання та виявлення академічного плагіату у науково-дослідній діяльності здобувачів вищої освіти і науково-педагогічних працівників Волинського національного університету імені Лесі Українки».

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 правдивої інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання учасники освітнього процесу 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, поставити запитання викладачеві.

Можливість визнання результатів навчання, отриманих у формальній, неформальній та інформальній освіті.

Здобувачеві 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 компонента, 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.

Можливість отримати додаткові (бонусні) бали. Здобувачі вищої освіти мають можливість додатково отримати бали за виконання індивідуальних завдань дослідницького характеру, зокрема, написання та опублікування наукових тез та статей з тематики ОК. Здобувачам, які брали участь у роботі конференцій, підготовці наукових публікацій, конкурсах студентських наукових робіт за тематикою ОК й досягли значних результатів, може бути присуджено додаткові (бонусні) бали, які зараховуються як результати поточного контролю. При цьому загальна кількість балів, що вноситься до відомості за поточну роботу не перевищуватиме 70 б.

Нарахування балів здійснюється освітнього компонента згідно з Таблицею Системи бонусних балів для здобувачів освіти

Системи бонусних балів для здобувачів освіти

Вид діяльності	Рівень / результат	Кількість бонусних балів
Студентські олімпіади	І місце	7
	ІІ місце	5
	ІІІ місце	3
	Участь в олімпіаді	2
Конкурси студентських наукових робіт	Диплом І ступеня	7
	Диплом ІІ ступеня	5
	Диплом ІІІ ступеня	3
Підготовка наукових публікацій	Публікація в WoS / Scopus	10
	Фахова стаття	7
	Нефахова стаття	5
	Публікація тез	2

Участь у конференціях	Виступ на конференції	2
Першість України з командного програмування	І місце	10
	ІІ місце	8
	ІІІ місце	6
	Участь	4

V. Підсумковий контроль

Оцінювання здійснюється згідно з Положенням про поточне та підсумкове оцінювання знань здобувачів освіти Волинського національного університету імені Лесі Українки. Форма підсумкового контролю – екзамен. Контрольні заходи включають поточний та підсумковий контроль. Екзамен виставляється за результатами поточного та підсумкового контролю роботи здобувачів освіти. Максимальна кількість балів, яку може набрати здобувач освіти за поточну навчальну діяльність з ОК, зокрема захист лабораторних робіт становить 70 балів.

Підсумковий модульний контроль здійснюється після завершення вивчення тем змістового модуля у формі виконання здобувачем освіти модульного контрольного завдання (тесту) та проводиться або під час навчального заняття. Максимальний бал, отриманий за модульні контрольні роботи, становить, не більше як 30 балів.

Підсумкова семестрова оцінка з ОК, виставляється без складання іспиту за результатами поточного і модульного контролю у випадку, якщо здобувач освіти успішно виконав усі завдання, передбачені силабусом, і набрав при цьому не менше як 75 балів. Така оцінка виставляється в день проведення екзамену в присутності здобувача освіти. Підсумкова семестрова оцінка у випадку складання іспиту визначається як сума поточної семестрової та екзаменаційної оцінок у балах. Отримана оцінка заноситься до електронного журналу успішності та індивідуального навчального плану студента.

У випадку незадовільної підсумкової семестрової оцінки, або за бажанням підвищити рейтинг, здобувач складає іспит у формі опитування та тестового контролю тощо. У цьому випадку на іспит виноситься 30 балів, а бали, набрані за результатами модульних контрольних робіт, анулюються.

Питання до екзамену

1. Поняття та принципи роботи Інтернет. Протокол HTTP.
2. Мова гіпертекстової розмітки HTML. Структура HTML-документа. Теги для роботи з текстом.
3. Мова гіпертекстової розмітки HTML. Теги для створення таблиць, малюнків та гіперпосилань.
4. Мова гіпертекстової розмітки HTML. Теги для створення форм на вебсторінках.
5. Використання каскадних таблиць стилів CSS. Поняття CSS, селектора, типи селекторів.
6. Синтаксис написання селекторів. Використання класів та ідентифікаторів.
7. Каскадні таблиці стилів CSS. Наслідування та каскадування.

8. Блочна структура вебсторінки. Особливості табличної та блочної верстки.
9. Семантична верстка HTML5.
10. Позиціонування елементів на вебсторінці.
11. Каскадні таблиці стилів CSS. Спеціальні селектори.
12. Каскадні таблиці стилів CSS. Псевдоелементи CSS та особливості їх використання при верстці вебсторінок.
13. Каскадні таблиці стилів CSS. Псевдокласи CSS та особливості їх використання при верстці вебсторінок.
14. JavaScript: призначення та можливості. Підключення .js-файлів. Способи уникнення передчасного виконання коду, типи даних, змінні та константи, оператори.
15. Основи скриптової мови програмування JavaScript: керуючі конструкції.
16. Масиви в JavaScript, методи для роботи з масивами.
17. Обробка даних форми в JavaScript.
18. Об’єкти в JavaScript, методи для роботи з об’єктами.
19. Поняття DOM-структури документа. Навігація в DOM.
20. Поняття DOM-структури документа. Властивості вузлів.
21. Поняття DOM-структури документа. Методи створення вузлів.
22. Події. Робота з мишею в JavaScript.
23. Події. Робота з клавіатурою в JavaScript.
24. PHP: призначення та можливості.
25. Поняття клієнт-серверної архітектури вебдодатку.
26. Основи мови програмування PHP: синтаксис, типи даних, змінні та константи, вирази, оператори.
27. Основи мови програмування PHP: керуючі конструкції.
28. Основи мови програмування PHP: функції для роботи з масивами.
29. Основи мови програмування PHP: функції для роботи з рядками.
30. Обробка даних форм в PHP. HTTP-запити.
31. Параметри URL.
32. Робота з файлами в PHP. Відкриття файлів, читання та запис даних в файл.
33. Сесії, робота з сесіями в PHP.
34. Cookies та робота з ними в PHP.
35. Робота з базою даних.
36. Класифікація вразливостей вебресурсів та атак на них.
37. Вимоги до захисту інформації вебсторінки від несанкціонованого доступу.
38. Поняття міжсайтового скриптинг (XSS).
39. Засоби захисту від XSS.
40. Поняття SQL-ін’єкції.
41. Засоби захисту від SQL-ін’єкції.
42. Атака на клієнта: підробка міжсайтових запитів (CSRF / XSRF).
43. Злом аутентифікації та сеансу. Clickjacking.
44. Міжсайтові запити CSRF.
45. Cookie атаки з перехоплення інформації.
46. Інструменти тестування уразливостей вебресурсів.
47. XXE (XML eXternal Entity)-атаки.
48. DDoS-атаки.
49. Поняття міжмережевого екрану.
50. Міжмережеві екрани для вебресурсів.
51. Використання інструментів захисту вебресурсів

52. Підходи до тестування вебресурсів.
53. Загальна характеристика методологій тестування безпеки: OSSTMM, PTES, OWASP Testing Guide.

VI. Шкала оцінювання

Шкала оцінювання знань здобувачів освіти з освітніх компонентів, де формою контролю є іспит

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
0–59	Незадовільно	Fx	Необхідне перескладання

VII. Рекомендована література та інтернет-ресурси.

1. Бородкіна І.Л., Бородкін Г.О. Web-технології та Web-дизайн : застосування мови HTML для створення електронних ресурсів. Київ, Ліра-К, 2020. 212 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. Куперштейн, Л. М., Притула, А. В., Маліновський, В. І. Аналіз технологій тестування на проникнення web-додатків. *Наукові праці Вінницького національного технічного університету*, 2024. №2. С.1-9.
5. Лаптон Е., Коул Філліпс Дж. Графічний дизайн: Нові основи. Київ, ArtHuss, 2020. 264 с.
6. Остапов С. Е., Євсеєв С. П., Король О.Г. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів, Новий Світ- 2000, 2020. 678 с.
7. Робін Вільямс. Дизайн. Книга для недизайнерів. Простою мовою про засади графічного дизайну. Харків, Vivat, 2022. 240 с.
8. Сучасний підручник з JavaScript. *JAVASCRIPT.INFO*. URL: https://uk.javascript.info/.

9. Фрімен Е., Робсон Е. Head First. Програмування на JavaScript. Харків, Фабула, 2022. 672 с.
10. Яцюк С. М., Юнчик В.Л. Web-дизайн. Безпека Web-ресурсів та додатків: навчальний посібник. Луцьк: ПП Іванюк, 2021. 316 с.
11. Andrew Hoffman. Web Application Security. Published by O'Reilly Media, Inc. 2020. 331 p.
12. CSS Підручник. Уроки для початківців. W3Schools українською *W3SchoolsUA.українською.* URL: https://w3schoolsua.github.io/css/index.html#gsc.tab=0
13. Drissi, Soufiane Zakaria. Cross-Site Scripting (XSS) Attacks and Penetration Testing, 2024. URL: https://www.researchgate.net/publication/383305348
14. HTML і CSS довідник українською. URL: https://html-css.co.ua/.
15. HTML Підручник. Початок. Уроки для початківців. W3Schools українською *W3SchoolsUA.українською*. URL: https://w3schoolsua.github.io/html/index.html.
16. Information Technology Laboratory. National Vulnerability Database. URL : https://nvd.nist.gov/vuln-metrics/cvss .
17. ISO/IEC 27001:2022Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/27001.
18. Kimminich B. Pwning OWASP Juice Shop. 422 p. URL: https://pwning.owasp-juice.shop/companion-guide/latest/
19. Laravel - The PHP Framework For Web Artisans. Laravel - The PHP Framework For Web Artisans. URL: https://laravel.com/
20. MITRE Common Weakness Enumeration. URL: https://cwe.mitre.org/.
21. OWASP Application Security Verification Standard (ASVS). URL: https://owasp.org/www-project-application-security-verification-standard//
22. PHP Підручник. Початок. Уроки для початківців. W3Schools українською *W3SchoolsUA.українською.* URL: https://w3schoolsua.github.io/php/index.html#gsc.tab=0.
23. PHP: Hypertext Preprocessor *PHP* URL: https://www.php.net/.