**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 – 2025

**Силабус нормативного освітнього компонента «**Технології веб розробки та захист вебресурсів**»** підготовки для першого (бакалаврського) рівня вищої освіти галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації.

**Розробники:**
Онищук Оксана Олександрівна, кандидат технічних наук, доцент кафедри комп'ютерних наук та кібербезпеки

**Погоджено**
Гарант освітньо-професійної програми:  Чернящук Н.Л.

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

протокол № 2 від 17 вересня 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,<br>125 Кібербезпека та захист інформації,<br>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</td></tr>
<tr><td colspan="2"></td><td>українська</td></tr>
</table>

## ІІ. Інформація про викладачів

ПІП – Онищук Оксана Олександрівна
Науковий ступінь – кандидат технічних наук
Вчене звання – доцент
Посада – доцент комп'ютерних наук та кібербезпеки
Контактна інформація: +38-0966943585, Onyshchuk.oksana@vnu.edu.ua
Дні занять: https://ps.vnu.edu.ua/cgi-bin/timetable.cgi

## ІІІ. Опис освітнього компонента

1. **Анотація.** Освітній компонент «Технології веб розробки та захист веб ресурсів» є нормативним та належить до циклу професійної підготовки освітнього ступеня бакалавр спеціальності 125 Кібербезпека та захист інформації, передбачає ознайомлення здобувачів вищої освіти із технологіями веб розробки, що використовуються під час програмування сучасних веб застосунків. Розглядаються верстка веб сторінок 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, умінь та навичок у сфері захисту веб ресурсів та особливостей проектування додатків з урахуванням можливих загроз.
2. **Мета і завдання освітнього компонента.** Сформувати у здобувачів вищої освіти компетентності із програмування веб застосунків 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.
3. **Результати навчання (Компетентності).**
   **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 житт

**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.

**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 / 20** |
| **Тема 1.** Поняття та принципи роботи Інтернет. Протокол HTTP. Мова гіпертекстової розмітки HTML. Базові конструкції та синтаксис мови HTML. | 10 | 2 | 3 | 4 | 1 | 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. | 10 | 2 | 3 | 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. | 10 | 2 | 3 | 4 | 1 | Звіт по лаб. роботі / 5 |
| **Тема 4.** Поняття DOM-структури документа. Навігація в DOM. Методи створення вузлів. Події в JavaScript. | 10 | 4 | 3 | 3 | | Звіт по лаб. роботі / 5 |
| Разом за модулем 1 | 40 | 10 | 12 | 15 | 3 | 20 |
| **Змістовий модуль 2. Програмування на PHP** | | | | | | **Т / 20** |
| **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. | 10 | 2 | 3 | 3 | 1 | Звіт по лаб. роботі / 6 |
| **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. | 9 | 2 | 3 | 3 | 1 | Звіт по лаб. роботі / 4 |
| **Тема 7.** Сесії та cookies | 8 | 2 | 2 | 3 | 1 | Звіт по лаб. роботі / 4 |
| **Тема 8**. Робота з базою даних. MySQL | 7 | 2 | 2 | 3 | | Звіт по лаб. роботі / 4 |
| **Тема 9**. Фреймворк Laravel. Створення додатків на Laravel | 7 | 2 | 2 | 3 | | Звіт по лаб. роботі / 4 |
| Разом за модулем 2 | 40 | 10 | 12 | 15 | 3 | 20 |
| **Змістовий модуль 3. Захист вебресурсів** | | | | | | **Т /30** |
| **Тема 10.** Класифікація вразливостей вебресурсів та атак на них. Вимоги до захисту інформації вебсторінки від несанкціонованого доступу. Нормативно-правова база. | 8 | 2 | 2 | 3 | 1 | Звіт по лаб. роботі / 6 |
| **Тема 11.** Міжсайтовий скриптинг (XSS) та засоби захисту від нього. SQL-ін'єкції та засоби захисту. Атака на клієнта: підробка міжсайтових запитів (CSRF / XSRF). | 8 | 2 | 2 | 3 | 1 | Звіт по лаб. роботі / 6 |
| **Тема 12.** Злом аутентифікації та сеансу. Clickjacking. Міжсайтові запити CSRF. Cookie атаки з перехоплення інформації. | 7 | 2 | 2 | 3 | | Звіт по лаб. роботі / 6 |
| **Тема 13.** Інструменти тестування уразливостей вебресурсів. XXE (XML eXternal Entity) - атаки. DDoS-атаки. Міжмережеві екрани для вебресурсів | 8 | 2 | 3 | 3 | | Звіт по лаб. роботі /6 |
| **Тема 14.** Використання інструментів захисту вебресурсів. Загальна характеристика методологій тестування безпеки: OSSTMM, PTES, OWASP Testing Guide. | 9 | 2 | 3 | 4 | | Звіт по лаб. роботі / 6 |
| Разом за модулем 3 | 40 | 10 | 12 | 16 | 2 | 30 |
| | | | | | | |
| Модульна контрольна робота 1 | | | | | | 15 |
| Модульна контрольна робота 2 | | | | | | 15 |
| **Всього годин/Балів** | **120** | **30** | **36** | **46** | **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 | 6 |
| 3 | 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 засуджені 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 "Технології веб розробки та захист веб ресурсів", розміщеного на платформі дистанційного навчання Moodle кафедри комп'ютерних наук та кібербезпеки, виконують всі завдання.

Прозвітуватися про виконання завдань можна, використовуючи електронний курс "Технології веб розробки та захист веб ресурсів", 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 освітнього компонента. 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 здобувачів освіти на території України чи поза її межами, для здобувачів освіти, 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 здобувач освіти під час поточного оцінювання за семестр –70 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за всі модульні контрольні роботи та індивідуальні завдання і складає 30 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 іспиту. В іншому випадку здобувач освіти складає іспит; максимальна кількість балів, яку можна отримати на іспиті – 30 балів, при цьому бали за підсумковий модульний контроль анульовуються.

Іспит проходить у письмовій формі.

### Питання, які виносяться на іспит

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.

**Білети на іспит складаються з трьох блоків:**

1. Тестові завдання: 20 запитань по 1 балу, всього 20 балів. Тестові завдання охоплюють всі теми змістових модулів.
2. Одне теоретичне запитання: 10 балів за повну відповідь. Охоплені теоретичні запитання всіх тем модулів.
3. Практичне завдання: всього 30 балів. Завдання готуються на основі завдань до лабораторних робіт та охоплюють всі теми лабораторних робіт.

***Приклад типового комплексного практичного завдання:***

1. За зразком створити форму з різними елементами управління. З допомогою JavaScript обробити отримані дані (15 балів).
2. З допомогою PHP забезпечити запис отриманих даних в базу даних (15 балів).

## VI. Шкала оцінювання

| **Оцінка в** | **Лінгвістична оцінка** | **Оцінка за шкалою ECTS** |
|---|---|---|

| **балах** | | **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 |

## 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. Andrew Hoffman. Web Application Security. Published by O'Reilly Media, Inc. 2020. 331 p.
11. CSS Підручник. Уроки для початківців. W3Schools українською *W3SchoolsUA.українською*. URL: https://w3schoolsua.github.io/css/index.html#gsc.tab=0
12. Drissi, Soufiane Zakaria. Cross-Site Scripting (XSS) Attacks and Penetration Testing, 2024. URL: https://www.researchgate.net/publication/383305348
13. HTML і CSS довідник українською. URL: https://html-css.co.ua/.
14. HTML Підручник. Початок. Уроки для початківців. W3Schools українською *W3SchoolsUA.українською*. URL: https://w3schoolsua.github.io/html/index.html.
15. Information Technology Laboratory. National Vulnerability Database. URL : https://nvd.nist.gov/vuln-metrics/cvss .
16. ISO/IEC 27001:2022Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/27001.
17. Kimminich B. Pwning OWASP Juice Shop. 422 p. URL: https://pwning.owasp-juice.shop/companion-guide/latest/
18. Laravel - The PHP Framework For Web Artisans. Laravel - The PHP Framework For Web Artisans. URL: https://laravel.com/
19. MITRE Common Weakness Enumeration. URL: https://cwe.mitre.org/.
20. OWASP Application Security Verification Standard (ASVS). URL: https://owasp.org/www-project-application-security-verification-standard//
21. PHP Підручник. Початок. Уроки для початківців. W3Schools українською

*W3SchoolsUA.українською.* URL: https://w3schoolsua.github.io/php/index.html#gsc.tab=0.
22. PHP: Hypertext Preprocessor *PHP* URL: https://www.php.net/.