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

СИЛАБУС
Вибіркового освітнього компонента
БЕЗПЕКА КЛІЄНТ-СЕРВЕРНОЇ ВЗАЄМОДІЇ У ВЕБСИСТЕМАХ
Підготовки другого (магістерського) рівня вищої освіти

Луцьк – 2026

Силабус вибіркового освітнього компонента “Безпека клієнт-серверної взаємодії у вебсистемах”. Підготовки другого (магістерського) рівня вищої освіти

Розробник:
Гаращенко Володимир Вікторович, старший викладач кафедри комп’ютерних наук та кібербезпеки

Погоджено

Гарант освітньо-професійної програми:  Булатецький В.В.

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

протокол № 6 від 15.01.2026 р.

Завідувач кафедри:  Гришанович Т. О.

І Опис навчальної дисципліни

Найменування показників	Характеристика навчальної дисципліни
	Вибіркова
Денна форма навчання	Рік підготовки 2
120/4 кредитів	Семестр 3
	Лекції 10 год.
	Лабораторні 14 год.
	Самостійна робота 88 год.
ІНДЗ: є	Консультації 8 год.
	Форма контролю: залік

ІІ Інформація про викладача

ПІП: Гаращенко Володимир Вікторович;
Посада: старший викладач кафедри комп'ютерних наук та кібербезпеки;
Контактна інформація: Harashchenko.Volodymyr@vnu.edu.ua
Дні занять: https://ps.vnu.edu.ua/cgi-bin/timetable.cgi?n=700

ІІІ. Опис освітнього компонента

Анотація курсу. Освітній компонент «Безпека клієнт-серверної взаємодії у вебсистемах» належить до переліку вибіркових освітніх компонентів. ОК «Безпека клієнт-серверної взаємодії у веб-системах» присвячений вивченню сучасних загроз вебзастосунків та методів їх запобігання на рівні взаємодії клієнта і сервера. У курсі розглядаються механізми автентифікації та авторизації на основі токенів, захист від міжсайтового виконання скриптів (XSS), обмеження доступу через політику CORS, протидія DDoS-атакам, використання проксі-серверів, а також безпечна обробка HTTP-запитів і заголовків.

Особлива увага приділяється практичним аспектам: налаштуванню захищених API, безпечному зберіганню та передачі даних, перевірці введення користувача, застосуванню сучасних стандартів веббезпеки та аналізу типових помилок розробників. У результаті навчання здобувачі набувають здатності проєктувати та реалізовувати захищену клієнт-серверну взаємодію у вебзастосунках.

Мета навчальної дисципліни. Формування у здобувачів знань і практичних навичок забезпечення безпеки клієнт-серверної взаємодії у вебсистемах шляхом застосування сучасних механізмів автентифікації, контролю доступу, захисту від вебуразливостей і мережевих атак, а також налаштування безпечної передачі даних між компонентами системи.

Soft skills:

- безпекове мислення (security mindset);
- аналіз ризиків та вразливостей;
- уважність до деталей при роботі з даними користувача;
- відповідальність за надійність програмних рішень;
- аргументація технічних рішень щодо безпеки;
- документування політик безпеки;
- прийняття рішень у кризових ситуаціях (інциденти, атаки);
- дотримання стандартів і best practices.

Структура освітнього компонента

Назви змістових модулів і тем	Кількість годин					Форма контролю / бали
	Усього	у тому числі				
		Лек.	Лаб.	Сам. роб.	Конс.	
Змістовий модуль 1. Безпека клієнт-серверної взаємодії у вебсистемах						
Тема 1. Основи безпеки клієнт-серверної взаємодії. Архітектура клієнт-серверних вебсистем та поверхня атаки. Класифікація загроз вебзастосунків і принципи secure-by-design. Модель ризиків і огляд OWASP.	10	2	2	6		Звіт по лаб. роботі /4
Тема 2. Автентифікація та авторизація у вебзастосунках Підходи session-based і token-based. Механізм JWT та OAuth 2.0/OpenID Connect. Безпечне зберігання секретів (Hashing, Salting) та багатофакторна автентифікація.	6		2	4		Звіт по лаб. роботі /4
Тема 3. Захист від ін'єкцій та XSS-вразливостей SQL та NoSQL ін'єкції. Механізми виникнення stored, reflected та DOM-XSS. Методи валідації, екранування і санітизації введення. Політика Content Security Policy та безпечна робота з DOM.	10	2	2	6		Звіт по лаб. роботі /4
Тема 4. Контроль міждоменної взаємодії Same-Origin Policy та механізм CORS. Безпечне налаштування API і запобігання CSRF-атакам. Аналіз типових помилок конфігурації доступу.	10	2	2	6		Звіт по лаб. роботі /4
Тема 5. Захист передачі даних і HTTP-політики безпеки HTTPS/TLS та захищені канали передачі. Security headers і безпечне використання cookies. Керування кешуванням і сесіями.	8		2	6		Звіт по лаб. роботі /4
Тема 6. Інфраструктурний захист вебсервісів Reverse proxy, API Gateway та приховування внутрішньої архітектури. Фільтрація трафіку, rate limiting і WAF. Балансування навантаження як механізм безпеки.	12	2	2	8		Звіт по лаб. роботі /4
Тема 7. Протидія атакам відмови в обслуговуванні Типи DDoS-атак і методи виявлення. Throttling, кешування і обмеження запитів. Моніторинг, Logging (SIEM системи) та стратегії Incident Response..	12	2	2	8		Звіт по лаб. роботі /4
Тест	8			8		Тестовий контроль знань / 16
Контрольна робота (розв'язування задач).	8			8		Контрольна робота (розв'язування задач)./16
ІНДЗ	16			16		Робота в групах/40
Всього годин/Балів	120	10	14	88	8	120 / 100 балів

Завдання для самостійного опрацювання

№ з/п	Тема	Кількість годин
1	Підготовка до лабораторних робіт	28
2	Підготовка до контрольних робіт	24
3	Опрацювання лекційного матеріалу	20
4	Виконання ІНДЗ	16
	Разом	88

IV. Політика оцінювання

Політика щодо академічної доброчесності. 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 (списування, плагіат, фабрикація), 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.

Комунікаційна політика. Здобувачі вищої освіти повинні мати активовану університетську пошту. Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту, можливе інше (додаткове) джерело комунікації, визначене викладачем для більш оперативного зв'язку зі студентами.

Політика щодо перескладання. Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).

Політика щодо оскарження оцінювання. Політика щодо оскарження оцінки. Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку згідно «Положення про порядок і процедури вирішення конфліктних ситуацій у Волинському національному університеті імені Лесі Українки»

Політика щодо відвідування занять. Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, академічна мобільність, які необхідно підтверджувати відповідними 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 проводитися у дистанційній формі за погодженням з керівником курсу та деканом факультету. Декан факультету видає розпорядження про дистанційне навчання на основі заяви здобувача. Під час дистанційного навчання лабораторні роботи виконуються відповідно до розкладу занять.

Навчання може здійснюватися за індивідуальним графіком відповідно до Положення про організацію освітнього процесу здобувачів освіти за індивідуальним графіком навчання у Волинському національному університеті імені Лесі Українки. Для цього здобувач подає заяву на ім'я декана, який, враховуючи успішність та підстави, погоджує або відхиляє подану заяву. У разі погодження здобувач освіти погоджує із викладачем план роботи, форми та терміни контролю. Індивідуальний графік затверджується на один семестр, а під час академічної мобільності – не більше ніж на рік.

Усі умови навчання в дистанційній формі та за індивідуальним графіком також подані у дистанційному курсі цього освітнього компоненту системи Moodle.

Бонуси. Після завершення вивчення курсу та перед початком екзаменаційної сесії здобувачам вищої освіти можуть бути нараховані додаткові бали за наукову діяльність. Такі бали надаються за участь у наукових конференціях, підготовку публікацій, здобуті результати в олімпіадах чи конкурсах студентських наукових робіт та інші досягнення у предметній галузі освітнього компонента. Порядок і систему нарахування бонусних балів визначає та затверджує науково-методична комісія факультету.

Визнання результатів навчання, отриманих у формальній, неформальній 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 на території України чи поза її межами, для здобувачів, 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».

Підсумковий контроль

Форма контролю – семестровий залік. Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе оцінювання всіх видів запланованої навчальної роботи протягом семестру: нараховується за якісне виконання лабораторних, контрольних, тестових контрольних робіт та виконання індивідуального завдання. Максимальна кількість балів, яку може отримати здобувач під час поточного оцінювання за семестр – 100 балів. Залік виставляється за результатами поточної роботи за умови, що здобувач освіти виконав ті види навчальної роботи, які визначено силабусом освітнього компонента.

У випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття (з поважних причин), на консультаціях він має право відпрацювати пропущені заняття та добрати ту кількість балів, яку було визначено на пропущені теми. У дату складання заліку викладач записує у відомість суму поточних балів, які здобувач освіти набрав під час поточної роботи.

У випадку, якщо здобувач освіти протягом поточної роботи набрав менше як 60 балів, він складає залік під час ліквідації академічної заборгованості. У цьому випадку бали, набрані під час поточного оцінювання анульовуються. Максимальна кількість балів на залік під час ліквідації академічної заборгованості, становить 100. На заліку, під час ліквідації академічної заборгованості, здобувач отримує комплексне завдання, яке охоплює всі теми і всі форми контролю, які пропонувалися при вивченні освітнього компонета.

Питання, які виносяться на залік під час ліквідації академічної заборгованості.

1. Основи безпеки клієнт-серверної взаємодії
2. Модель взаємодії клієнт-сервер у вебі та її поверхня атаки.
3. Типові загрози веб-застосунків і принципи безпечної розробки. Огляд OWASP.
4. Автентифікація та авторизація на основі токенів
5. Session-based та token-based підходи. JWT, refresh-tokens, зберігання токенів і їх життєвий цикл.
6. Загрози викрадення токенів та методи захисту.
7. Захист від XSS та небезпечного введення
8. Типи XSS-атак (stored, reflected, DOM).
9. Екранування, санітизація та Content Security Policy.
10. Безпечна робота з HTML та JavaScript у клієнті.
11. Політика однакового походження та CORS
12. Same-Origin Policy і її обмеження.
13. Налаштування CORS для API та типові помилки конфігурації.
14. Захист від CSRF і небезпечних міждоменних запитів.
15. HTTP-заголовки безпеки та захист передачі даних
16. HTTPS, TLS і захищена передача даних.
17. Security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options).
18. Cookies, SameSite та безпечне кешування.
19. Проксі, шлюзи та фільтрація трафіку
20. Reverse proxy, API Gateway та балансування навантаження.
21. Приховування внутрішньої інфраструктури та фільтрація запитів.
22. Rate limiting і WAF.
23. Протидія DDoS та моніторинг інцидентів.
24. Типи DDoS-атак і методи їх виявлення.
25. Обмеження запитів, throttling та кешування. Логування, аудит і реагування на інциденти безпеки.

Комплексне завдання на залік під час ліквідації академічної заборгованості:

1. На ліквідацію академічної заборгованості здобувач повинен принести ІНДЗ (максимальні кількість балів 40).

2. Виконання тестових завдань, які охоплюють всі запитання, які виносяться на залік під час ліквідації академічної заборгованості. 30 запитань по 1 балу (максимальні кількість 30 балів)
3. Три задачі по 10 балів кожна. Створити вітку на GitHab в репозиторії освітнього компонента. У вітку закинути виконані завдання.

V. Шкала оцінювання

Оцінка в балах за всі види навчальної діяльності	**Оцінка**
90 – 100	Відмінно
82 – 89	Дуже добре
75 - 81	Добре
67 -74	Задовільно
60 - 66	Достатньо
1 – 59	Незадовільно

VI. Рекомендована література та інтернет-ресурси

1. Безпека Веб-додатків. *Seeton*. URL: https://www.seeton.pro/cybersecurity/waf-rasp/ (дата звернення: 13.02.2026).
2. Stfalcon E. Як забезпечити безпеку веб-додатків: найкращі практики | Stfalcon. *Logistics & Transportation Software Development Agency | Stfalcon*. URL: https://stfalcon.com/uk/blog/post/building-secure-web-applications-best-practices-and-strategies (дата звернення: 13.02.2026).
3. Owasp це про поліпшення безпеки онлайн веб-додатків. *FoxmindEd*. URL: https://foxminded.ua/owasp-tse/ (дата звернення: 13.02.2026).

HYPERLINK "https://cert.gov.ua/recommendation/19" \n