Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативної навчальної дисципліни

ТЕХНОЛОГІЯ ПРОГРАМУВАННЯ ЗАХИЩЕНИХ СИСТЕМ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека (2020 р.)
Форма навчання	Денна
Розробник (викладач)	Прус Руслана Богданівна, кандидат технічних наук
Контактна інформація	prus.ruslana@vnu.edu.ua
Програма навчальної дисципліни	Програма навчальної дисципліни розміщена на сторінці кафедри комп'ютерних наук та кібербезпеки на офіційному сайті ВНУ імені Лесі Українки
Семестр, курс	7 семестр, 4 курс
Обсяг дисципліни	Загальний обсяг: 120 годин, 4 кредити Аудиторних занять: 54, з них 24 лекції, 30 лабораторні роботи Самостійна робота: 58 години Консультації: 8 год.
Форма контролю	Залік
Час занять	Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Мова навчання	Українська
Анотація дисципліни	Даний курс знайомить студентів з теорією та методами безпечного програмування з метою розв'язування прикладних задач та створення програмного забезпечення систем ІБ; етапами життєвого циклу розробки безпечного програмного забезпечення; методами розробки алгоритмів, лінійними та ієрархічними структурами даних та алгоритмів їх обробки; основами процедурного та об'єктно-орієнтованого програмування із застосуванням принципів безпечного програмування. Студенти навчаються застосовувати сучасні технології безпечного програмування в системах інформаційної та кібербезпеки; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування та вразливостей; обирати методи зберігання та ефективні алгоритми обробки для відповідних структур даних для створення захищених програм; виконувати модифікацію програм, додаючи, змінюючи або усуваючи окремі їх компоненти з метою зміни їх функцій; застосовувати прийоми проектування та створення власних захищених програм; виконувати аналіз програмного коду. Розглядаються основи програмування захищених веб-сайтів та засоби серверної безпеки рівня веб-серверу, бази даних, засобів авторизації та аутентифікації користувачів.
Мета вивчення дисципліни	Метою викладання навчальної дисципліни «Технологія програмування захищених систем» є засвоєння студентами фундаментальних знань в області теорії і практики програмування із застосуванням процедурної та об'єктна-орієнтовної технологій програмування.

	Завдання навчальної дисципліни полягає у формуванні теоретичних знань та практичних умінь у сфері розробки безпечного програмного забезпечення, побудови та аналізу алгоритмів з використанням методів створення ефективних програм на базі відповідних структур даних та алгоритмів їх обробки для систем інформаційної та кібернетичної безпеки.
Результати навчання	*Загальні компетентності:* • Здатність застосовувати знання у практичних ситуаціях. • Знання та розуміння предметної області та розуміння професії. • Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. • Здатність до пошуку, оброблення та аналізу інформації *Фахові компетентності:* • Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) • Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою *Програмні результати навчання:* • Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності • Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах • Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем • Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем • Вирішувати задачі аналізу програмного коду на наявність можливих загроз

Структура навчальної дисципліни

Назви змістових модулів і тем	Усього	Лек.	Лаб.	Сам. роб.	Конс.	Бали
1	120	24	30	58	8	100
Змістовий модуль 1. Технологія розробки безпечного програмного забезпечення						
Тема 1. Основні принципи безпечного програмування 1. Життєвий цикл розробки програмного забезпечення (ПЗ) 2. Програмування захищених пристроїв 3. Характеристика технології .Net Framework 4. Дані програми. Безпека даних.	8	2	2	4		3

5. Управління потоком виконання програми.						
Тема 2. Технологія структурного процедурного програмування 1. Структурний підхід в програмуванні. Структуровані типи даних 2. Розбиття програми на підпрограми. Методи.	7	2	2	3		3
Тема 3. Технологія об'єктно-орієнтованого програмування 1. Принципи об'єктно-орієнтовного програмування. Класи та об'єкти. 2. Похідні класи. Класи збереження даних	8	2	2	3	1	3
Тема 4. Засоби безпеки бази даних 1. Базові можливості мови SQL. 2. Маніпулювання даними та перетворення їх типів. Використання під запитів для отримання даних. 3. Базові можливості мови SQL для модифікації даних. 4. Адміністрування баз даних. 5. Права та ролі користувачів. Role-based user access control.	9	2	2	4	1	3
Тема 5. Створення базових елементів графічного інтерфейсу користувача 1. Проектування та розробка основних компонент графічного інтерфейсу користувача (GUI). 2. Класи стандартних елементів управління бібліотеки класів Windows Forms	9	2	2	4	1	3
Тема 6. Розробка додатків в інтегрованих середовищах. Побудова керованого та захищеного коду за допомогою Windows Forms, ADO.NET, WPF, ASP.NET 1. Засоби збереження даних. DataGrideView, DB. 2. Засоби для створення веб-додатків - ASP.NET	9	2	2	4	1	3
Разом за модулем 1	**50**	**12**	**12**	**22**	**4**	18
Змістовий модуль 2. Практичні аспекти розробки захищених веб-ресурсів						
Тема 7. Особливості побудови та розгортання сучасного веб-сайту на базі системи управління вмістом (CMS).	8	2	2	3	1	3

Тема 8. Засоби безпеки рівня серверної інфраструктури. Особливості застосування технології віртуалізації рівня операційної системи.	8	2	2	4		3
Тема 9. Архітектура веб-систем. Об’єкти захисту/атаки. Аутентифікація та авторизація.	8	2	2	3	1	3
Тема 10. Взаємодія між веб-сервісами. REST-інтерфейс та його безпека.	7	2	2	3		3
Тема 11. Відкритий проект по забезпеченню безпеки веб-додатків (OWASP).	7	2	2	3		2
Тема 12. Вразливості веб-ресурсів та додатківта атаки на них. Міжсайтовий скриптинг (XSS) та засоби захисту від нього. SQL-ін’єкції: характеристика вразливості та засоби захисту.	7	1	2	3	1	3
Тема 13. Основи методології та безпеки веб-ресурсів та додатків. Загальна характеристика методологій тестування безпеки: OSSTMM, PTES, OWASP Testing Guide.	7	1	2	3	1	3
Разом за модулем 2	**52**	**12**	**14**	**22**	4	20
Модульна контрольна робота №1	6		2	4		10
Модульна контрольна робота №2	6		2	4		10
Залік	6			6		40
Разом за 7 семестр:	**120**	**24**	**30**	**58**	8	100

Оцінювання

При вивченні дисципліни студент виконує такі види робіт: опрацювання теоретичного матеріалу та виконання лабораторних робіт, виконання індивідуальних завдань, написання тестів.

Рівень знань студента оцінюється в балах, фіксується в журналі після вивчення змістового модуля. Підсумкова оцінка за національною шкалою за семестр заноситься в заліково-екзаменаційну відомість.

Усі види навчальної діяльності студента оцінюються певною кількістю балів. Підсумковий контроль здійснюється у формі заліку. Сумарна кількість балів, яку студент отримує при засвоєнні змістових модулів за 100-бальною шкалою, визначає його підсумкову оцінку.

Дисципліна складається з двох змістових модулів. Підсумкова оцінка за 100-бальною шкалою складається із сумарної кількості балів за:

1. поточне оцінювання (максимум 40 балів);
2. залік (максимум 60 балів).

Поточний контроль, який має на меті перевірку рівня знань студента, здійснюється викладачем упродовж семестру у межах змістових модулів. Поточний контроль включає оцінку

поточної роботи студента у ході виконання лабораторних робіт. Максимальна кількість балів за результатами поточного контролю становить 40 балів.

Підсумковий контроль, який здійснюється викладачем, має на меті перевірку рівня знань студента під час виконання залікового тесту, виконання практичного завдання та усної відповіді. Максимальна кількість балів, яку студент може набрати за залік, становить 60 балів, з яких по 10 балів – це оцінка за кожну із двох модульних контрольних робіт.

Поточний контроль (мах = 40 балів)		**Модульний контроль/залік (мах = 60 балів)**			**Загальна кількість балів**
Змістовий модуль 1	**Змістовий модуль 2**	**МКР 1**	**МКР 2**	**Залік**	
20	20	10	10	40	100

Підсумковий контроль

Залік складається з трьох частин: 1) написання залікового тесту (максимум – 20 балів); 2) виконання практичного завдання (максимум 10 балів) та 3) усна відповідь (максимум – 10 балів).

В оцінці знань студентів враховується:

1) достатність обсягу відповіді (повна, недостатньо повна, неповна);

2) обізнаність з основними поняттями, принципами, законами, правилами навчальної дисципліни;

3) логічність викладу матеріалу;

4) обґрунтованість власних міркувань;

5) уміння інтегрувати та диференціювати знання теоретичного матеріалу та застосовувати їх при виконанні практичних завдань.

Відповідь вважається *повною* (*40 балів*), якщо студент повністю оволодів матеріалом, обізнаний з усіма поняттями і термінами навчального курсу і адекватно оперує ними під час відповідей на поставлені питання, а також посилається на наукові дослідження з навчальної дисципліни, ознайомлений зі спеціальною літературою; демонструє здатність аналізувати факти, аргументувати власні судження теоретичними і фактичними положеннями, підсумувати сказане висновками.

Відповідь вважається *недостатньо повною* (*36 балів*) за умов непоганого володіння знаннями з навчального предмету. Відповідь студента має бути правильною й обгрунтованою. Студент повинен продемонструвати знання теоретичного матеріалу, навички самостійної навчально-пізнавальної діяльності, здатність викладати матеріал в певній логічній послідовності. Допускаються незначні помилки, які не впливають на загальне розуміння викладеного матеріалу.

Відповідь вважається *неповною* (*32 бали*), якщо продемонстровані знання з предмету носять фрагментарний і поверхневий характер. Теоретичні і фактичні знання відтворюються репродуктивно, без глибокого осмислення, аналізу, порівняння, узагальнення. Студент обізнаний з літературними джерелами з навчальної дисципліни, але не може дати достатньо критичної їх оцінки; допускає суттєві помилки, які порушують логіку викладення матеріалу.

Залік вважається *нескладеним (нижче 24 балів),* за умов неправильної або неповної відповіді, яка свідчить про нерозуміння поставленого завдання. Студент не володіє понятійно-категоріальним апаратом, необізнаний з джерельною базою з навчальної дисципліни і допускає грубі помилки у викладенні матеріалу.

Політика викладача щодо студента

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; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування.

Очікується, що всі студенти відвідають усі лекції і практичні 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 у встановлені викладачем терміни під час консультацій.

Перескладання модулів відбувається із дозволу викладача за наявності поважних причин (наприклад, лікарняний).

Рекомендована література та інтернет-ресурси

1. Certified Information Systems Security Professional Study Guide – USA.: CISSP, 2015 – 901 с.
2. Chris Snyder. Pro PHP Security: From Application Security Principles to the Implementation of XSS Defenses – USA.: Amazon DS, 2010 – 368 с.
3. Jeremiah Grossman. XSS Attacks CROSS SITE SCRIPTING EXPLOITS AND DEFENSE. – USA.: Amazon DS, 2018 – 630 с.
4. Jonathan LeBlanc. Identity and Data Security for Web Development: Best Practices – UK.: O'Reilly Media, 2016 – 204 с.
5. Kimberly Graves. CEH: Official Certified Ethical Hacker Review Guide. – USA: EC- Council, 2007. – 264 с.
6. Martin Kleppmann Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems Paperback. – O'Reilly Media, 2016 – 400 p.
7. 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.
8. Створення та обробка баз даних: навч. посібник для студ. техн. спец. вищ. навч. закл. / Л. С. Глоба, М. Ю. Тернова, Р. Л. Новогрудська, О. С. Штогрина. Київ:НТУ України «КПІ», 2013. 477 с.
9. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. – СПб.: Питер, 2020. – 448 с.

10. Holistic Info-Sec for Web Developers. [Electronic resource]. – Access mode: https://holisticinfosecforwebdevelopers.com/
11. OWASP Web Security Testing Guide. [Electronic resource]. – Access mode : https://owasp.org/www-project-web-security-testing-guide/
12. Open Web Application Security Project [Електронний ресурс]. Режим доступу: www.owasp.org
13. Топ-10 OWASP-2017 Десять самых критичных угроз безопасности веб-приложений. [Електронний ресурс] – Режим доступу: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017-ru.pdf