СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«АНАЛІЗ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**Ступінь освіти**	бакалавр
	Галузь знань	12 Інформаційні технології
	Тривалість викладання	13, 14 чверті
	Заняття:	Осінній семестр
	лекції:	2 години
	практичні заняття:	1година
	Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»:
https://do.nmu.org.ua/course/view.php?id=4235

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладача

Сафаров Олександр Олександрович	к.т.н., доцент
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/saforov.php
E-mail:	safarov.o.o@nmu.one

1. Анотація до курсу

Студенти отримують теоретичні знання і практичні навички з основних принципів побудови та функціонування захищеного програмного забезпечення; одержують знання про методи реалізації систем захисту для програмного забезпечення.

2. Мета та завдання курсу

Мета дисципліни – опанування основними термінами та категоріями безпеки програмного забезпечення, принципами і засобами здійснення аналізу та власне забезпечення цієї безпеки в інформаційних системах з урахуванням сучасного стану та прогнозу розвитку методів та засобів здійснення погроз зі сторони потенційних порушників.

Завдання курсу полягає у формуванні здатності здобувачів вищої освіти обґрунтовано використовувати знання щодо забезпечення безпеки програмного забезпечення у професійній сфері на основі системного підходу.

3. Результати навчання

Володіти знаннями щодо технологій захисту програмного забезпечення та принципами побудови систем захисту для програмних додатків.

Застосовувати в практичній діяльності механізми захисту, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності в програмних додатках.

Вирішувати задачі у сфері безпеки програмного забезпечення з використанням нормативно-правової бази України та міжнародного законодавства.

4. Структура курсу

ЛЕКЦІЇ

Змістовний модуль №1

1. Основні поняття, визначення, закони
2. Основні загрози безпеки
3. Механізми реалізації безпеки
4. Забезпечення безпеки об'єктів інформаційної сфери держави
5. Характеристика стандартів із забезпечення інформаційної безпеки
6. Ризик роботи на персональному комп'ютері
7. Засоби захисту інформації
8. Загальна характеристика комплексного захисту інформації

ПРАКТИЧНІ ЗАНЯТТЯ

1.Розмежування повноважень користувачів на основі парольної аутентифікації.

2.Логування дій користувачів у програмних системах.

3.Методи захисту програмного забезпечення.

4.Захист веб-ресурсів від ботів та спаму за допомогою механізму CAPTCHA

5.Аналіз захищеності веб-ресурсів

6.Особливості захисту даних за допомогою технології Blockchain

5. Технічне обладнання та/або програмне забезпечення

Необхідний доступ до системи дистанційного навчання НТУ «ДП». Активований акаунт університетської пошти (student.i.p.@nmu.one) на Офіс365.

Технічне обладнання до практичних робіт:

№ роботи	Назва роботи	Інструменти, обладнання та програмне забезпечення, що застосовуються при проведенні роботи
1	Розмежування повноважень користувачів на основі парольної аутентифікації.	Середовище розробки для мов програмування Python, C\C++, JavaScript
2	Логування дій користувачів у програмних системах.	Середовище розробки для мов програмування Python, C\C++, JavaScript

№ роботи	Назва роботи	Інструменти, обладнання та програмне забезпечення, що застосовуються при проведенні роботи
3	Методи захисту програмного забезпечення	Середовище розробки для мов програмування Python, C\C++, JavaScript
4	Захист веб-ресурсів від ботів та спаму за допомогою механізму CAPTCHA	Середовище розробки для мов програмування Python, C\C++, JavaScript
5	Аналіз захищеності веб-ресурсів	Інструментарій для аналізу системи KaliLinux
6	Особливості захисту даних за допомогою технології Blockchain	Середовище розробки для мов програмування Python, C\C++, JavaScript

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74 -89	добре
60-73	задовільно
0-59	незадовільно

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Практична частина		Бонус	**Разом**
	При своєчасному складанні	При несвоєчасному складанні		
55	45	30	0	**100**

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи. Теоретична частина оцінюється за результатами здачі іспиту. Кожний білет містить 2 питання.

6.3. Критерії оцінювання підсумкової роботи

Робота повинна містити розгорнуті відповіді на два питання білету. Якщо робота виконується у дистанційному режимі, то видача номеру білета проходить через систему MS Teams у зазначеній викладачем групі спілкування. В такому режимі виконана робота пишеться вручну, фотографується та відсилається не електронну

пошту викладача у впродовж встановленого викладачем часу. За виконану роботу нараховуються бали:

55 бали – дана розгорнута відповідь на два питання;

40 балів – дана розгорнута відповідь на одне питання, але є помилки при розгляді іншого питання, або є несуттєві помилки у відповідях на два питання;

25 балів – дана повна відповідь на одне питання або на два питання зі значними помилками;

15 балів – відповідь на одне питання із значними помилками;

0 балів – відповіді на питання відсутні або повністю невірні, або робота здана несвоєчасно.

6.4. Критерії оцінювання практичної роботи

З кожної практичної роботи здобувач вищої освіти отримує запитання з переліку контрольних запитань до роботи.

15 балів – Достатня зрозумілість відповіді

10 бали – Добра зрозумілість відповіді

7 бали – Задовільна зрозумілість відповіді

0 балів – Незадовільна зрозумілість відповіді

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. 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). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". https://cutt.ly/IBesJEc.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

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

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, 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 (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

8 Рекомендовані джерела інформації

8.1. Основні

1. Горбенко В. І., Лісняк А. О. Безпека програм та даних : навчальний посібник для здобувачів ступеня вищої освіти бакалавра спеціальності 121 «Інженерія програмного забезпечення» освітньо-професійної програми «Програмна інженерія». Запоріжжя : ЗНУ, 2022. 72 с.
2. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. – К.: Видавництво НА СБ України, 2020. – 256 с.
3. Цибульник, С. О. Технології розроблення програмного забезпечення. Частина 1. Життєвий цикл програмного забезпечення [Електронний ресурс] : підручник для здобувачів ступеня бакалавра за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології» / Цибульник С. О., Барандич К. С. ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 3,43 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 270 с. – Назва з екрана.
4. Andress J. Foundations of information security: a straightforward introduction. San Francisco : No Starch Press, 2019. 222 p
5. Richards M. Fundamentals of Software Architecture: An Engineering Approach / M. Richards, N. Ford. – Sebastopol: O'Reilly Media, 2020. – 432 p

8.2. Допоміжні

1. Nadalin Alessandro. WASEC: Web Application Security for the everyday software engineer: Everything a web developer should know about application security: concise, condensed and made to last/ A. Nadalin. — Leanpub, 2020. — 161 p.— ISBN 1670062449, 9781670062444.

8.3. Інформаційні ресурси

1. https://zakon.rada.gov.ua
2. Пошукова система у базі лекцій, наукових статей, навчальних посібників та підручників з усього світу/GoogleАкадемія - Режим доступу до ресурсу: http://scholar.google.com.ua/