СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**Ступінь освіти**	бакалавр
	Галузь знань	12 Інформаційні технології
	Тривалість викладання	11, 12 чверті
	Заняття:	Весняний семестр
	лекції:	2 години
	практичні заняття:	1 година
	Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»:
https://do.nmu.org.ua/course/view.php?id=4014

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладачів

Котух Євген Володимирович	д.т.н., професор
Персональна сторінка	https://bit.nmu.org.ua/staff/kotuh/
E-mail:	Kotukh.Ye.V@nmu.one

Мілінчук Юлія Анатоліївна	асистент
Персональна сторінка	https://bit.nmu.org.ua/staff/milinchuk/
Е-пошта:	milinchuk.yu.a**@nmu.one**

1. Анотація до курсу

Дисципліна «Захист інформації в інформаційно-комунікаційних системах» входить до складу вибіркових дисциплін більшості спеціальностей 12 галузі знань «Інформаційні технології». Вона присвячена розгляду стандартів, методів та засобів проектування, впровадження та підтримки захищених інформаційних систем. В курсі розглядаються сучасні підходи до забезпечення захисту інформаційних активів,

приділяється певна увага процесам оцінки захищеності систем і технологій обробки інформації. Розглянуті складові комплексних систем захисту інформації. Надані певні відомості про методи протидії актуальним кіберзагрозам.

2. Мета та завдання курсу

Мета дисципліни – формування компетентностей щодо використання сучасних процедур забезпечення безпеки інформації, формування політики безпеки інформації в ІКС, застосовування нормативно-правових, організаційних та технічних процедури забезпечення безпеки інформації в корпоративних мережах.

Завдання курсу:

- ознайомити здобувачів вищої освіти з певними практиками побудови та використання захищених інформаційних систем;
- вивчити особливості реалізації систем захисту у гетерогенному інформаційному середовищі;
- закріпити знання та навички з адміністрування та експлуатації інформаційно-телекомунікаційних систем;
- навчити здобувачів вищої освіти використовувати вітчизняні та міжнародні стандарти і нормативні документи з метою побудови кіберстійких рішень.

3. Результати навчання

Основні результати навчання:

– вміти використовувати стандартні методи аналізу захищеності систем та технологій обробки інформації, створювати моделі загроз, порушника в інформаційних та інформаційно-комунікаційних системах;

– вміти використовувати мережні технології в процесі проектування захищеного програмного забезпечення;

– надавати обґрунтований опис систем забезпечення захисту інформації, як складових інформаційних систем, що проектуються;

– обґрунтовано використовувати процедури вибору захищених рішень в процесі створення і використання інформаційних систем та технологій.

4. Структура курсу

ЛЕКЦІЇ

Змістовний модуль №1

1. Правові та організаційні засади захисту інформації в інформаційно-комунікаційних системах.
2. Засоби антивірусного захисту інформації у інформаційно-комунікаційних системах.
3. Програмні методи та засоби захисту інформації у інформаційно-комунікаційних системах.
4. Криптографічні методи захисту інформації при її передаванні у інформаційно-комунікаційних системах.
5. Створення, введення в дію та супроводження захищених систем.

Змістовний модуль №2

4. Законодавчий та адміністративний рівні інформаційної безпеки

5. Законодавство України про захист інформації в телекомунікаційних системах та мережах

5.1 ЗаконодавствоУкраїни в галузі інформаційної безпеки

5.2 Огляд міжнародних стандартів у галузі інформаційної безпеки.

ПРАКТИЧНІ ЗАНЯТТЯ

1. . Оцінка ризиків інформаційної безпеки.

2. Розробка моделей порушника та загроз.

3 . Розробка політики безпеки інформації в інформаційних системах.

4. Вирішення практично-ситуаційних задач у сфері безпеки інформації з використанням нормативно-правової бази України та міжнародного законодавства.

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	Оцінка ризиків інформаційної безпеки.	Персональний комп'ютер Платформа MS Windows або Ubuntu MS Office, або MS Office 365
2	Розробка моделей порушника та загроз.	Персональний комп'ютер Платформа MS Windows або Ubuntu MS Office, або MS Office 365
3	Розробка політики безпеки інформації в інформаційних системах	Персональний комп'ютер Платформа MS Windows або Ubuntu MS Office, або MS Office 365
4	Вирішення практично-ситуаційних задач у сфері безпеки інформації з використанням нормативно-правової бази України та міжнародного законодавства	Доступ до електронного ресуру https://zakon.rada.gov.ua

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		
60	40	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:

60 бали – дана розгорнута відповідь на два питання;

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

30 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.

10 балів – Достатня зрозумілість відповіді

7 бали – Добра зрозумілість відповіді

5 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 заняття проводяться в асинхронному режимі. Проводиться запис занять. При відсутності на занятті здобувач вищої освіти має опрацювати матеріал самостійно.

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. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
2. Інформаційна безпека держави : підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.] ; в 2 т. – Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2016. – 264 с.
3. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп’ютерних системах: підручник. – Ніжин: ФОП Лук’яненко В.В., ТПК «Орхідея», 2020. – 236с.
4. Інформаційна безпека в комп’ютерних мережах: навч. посіб. / О.А. Смірнов, О.К. Конопліцька-Слободенюк, С.А. Смірнов [та ін.]; М-во освіти і науки

України, Центральноукраїн. нац. техн. ун-т. – Кропивницький: Лисенко В.Ф., 2020. – 295 с.
5. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
6. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в КС від НСД
8. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в КС від НСД

8.2. 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/**