СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ОСНОВИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**Ступінь освіти**	бакалавр
	Галузь знань	12 Інформаційні технології
	Тривалість викладання	5,6 чверті
	Заняття:	Осінній 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=2535

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладачів

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

Мілінчук Юлія Анатоліївна	асистент
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/milinchuk.php
E-пошта:	milinchuk.yu.a@**nmu.one**

1. Анотація до курсу

Студенти отримують теоретичні знання і практичні навички з основних принципів побудови та функціонування систем інформаційної безпеки на рівні людини, суспільства та держави; одержують знання про архітектуру побудови системи інформаційної безпеки, функціональні можливості модулів інформаційної безпеки та їх управління.

2. Мета та завдання курсу

Мета дисципліни – опанування основними термінами та категоріями безпеки інформації, принципів і засобів забезпечення особистої інформаційної безпеки та безпеки в інформаційних системах на підприємствах, організаціях та установах на рівні їх відтворення для практичного застосування у процесі діяльності майбутнього спеціаліста з кібербезпеки.

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

3. Результати навчання

Володіти знаннями щодо технологій захисту інформації та принципами побудови систем захисту інформації.

Застосовувати в практичній діяльності механізмів захисту, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій.

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

4. Структура курсу

ЛЕКЦІЇ

Змістовний модуль №1

1. Поняття інформаційної безпеки.
1.1 Поняття інформаційної безпеки
1.2 Загрози інформаційної безпеки
1.3 Порушники інформаційної безпеки
2. Організаційний та технічний рівні інформаційної безпеки
2.1 Основні класи заходів організаційного рівня
2.2 Фізичні засоби захисту
2.3 Криптографічні засоби захисту
3. Система забезпечення інформаційної безпеки
3.1 Теоретичні основи побудови систем безпеки.
3.2 Моделі безпеки інформаційних систем

Змістовний модуль №2

4. Законодавчий та адміністративний рівні інформаційної безпеки
4.1 Огляд законодавства в галузі інформаційної безпеки
4.2 Огляд міжнародних стандартів у галузі інформаційної безпеки.

ПРАКТИЧНІ ЗАНЯТТЯ

1. Генерація псевдовипадкових послідовностей за допомогою конгруентного генератора. Визначення можливості їх застосування у криптографічних перетвореннях.

2. Генерація псевдовипадкових послідовностей за допомогою лінійного рекурентного регістру зсуву. Визначення можливості їх застосування у криптографічних перетвореннях.

3. 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	Генерація псевдовипадкових послідовностей за допомогою конгруентного генератора. Визначення можливості їх застосування у криптографічних перетвореннях.	Компілятор C\C++
2	Генерація псевдовипадкових послідовностей за допомогою лінійного рекурентного регістру зсуву. Визначення можливості їх застосування у криптографічних перетвореннях.	Компілятор C\C++
3	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		
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. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем/ М.В.Гайворонський, О.М. Новіков.–К.: Видавнича група BHV,2009. – 608 с., іл
2. Юдін О.К., Конахович Г.Ф., Корченко О.Г., Захист інформації в мережах передачі даних: підручник/О.К. Юдін, Г.Ф.Конахович, О.Г.Корченко. – К.:Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. –714с., іл.
3. Богуш В.М., Довидьков О.А. Основи захищених інформаційних технологій/ В.М.Богуш, О.А.Довидьков. –К.: ДУІКТ, 2005. –450 с.

8.2. Допоміжні

1. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. –К.: МК-Прес, 2005.–432 с.
2. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. –К.: ДУТ, 2015. –288 с.
3. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак; під ред. В.О. Хорошко.–Луганськ: Ноулідж, 2012.–480 с.

8.3. Інформаційні ресурси

1. https://zakon.rada.gov.ua

2. Пошукова система у базі лекцій, наукових статей, навчальних посібників та підручників з усьогосвіту / GoogleАкадемія - Режим доступу до ресурсу: http://scholar.google.com.ua/