СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ОСНОВИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**Ступінь освіти**	бакалавр
	Освітня програма	Кібербезпека
	Тривалість викладання	3,4 чверті
	Заняття:	Весінній 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

Викладач:
Тимофєєв Дмитро Сергійович
Старший викладач кафедри безпеки інформації та телекомунікацій

Персональна сторінка
https://bit.nmu.org.ua/ua/pro_kaf/prepods/timofeev.php
E-mail: tymofieiev.d.s@nmu.one

1. Анотація до курсу

«Основи забезпечення безпеки інформації» є дисципліною, яка сприяє підготовці фахівців у сфері кіберзахисту. Студенти отримують теоретичні знання і практичні навички з основоположних принципів побудови та функціонування системи інформаційної безпеки на рівні людини, суспільства та держави; одержують знання про архітектуру побудови системи інформаційної безпеки, функціональні можливості модулів інформаційної безпеки та їх управління. По завершенню вивчення дисципліни студенти можуть обґрунтовано використовувати знання щодо забезпечення безпеки інформації у професійній сфері на основі системного підходу

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:

– ознайомити здобувачів вищої освіти із теоретичними знаннями щодо взаємозв'язків безпеки інформації, інформаційної безпеки, кібербезпеки та захисту інформації;

– ознайомити здобувачів вищої освіти з технологіями захисту інформації та принципами побудови систем захисту інформації;

– ознайомити здобувачів вищої освіти з критеріями вибору технології та систем захисту інформації, що є найбільш ефективними для вирішення конкретних задач;

– ознайомити здобувачів вищої освіти з механізмами захисту, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій;

– ознайомити здобувачів вищої освіти збазовими знаннямищодо інформаційного протиборства, інформаційної війни, гібридної війни та спеціальних інформаційних операцій;

– ознайомити здобувачів вищої освіти з нормативно-правовими актами України та міжнародних стандартів в частині, що регулюють інформаційні відносини та оцінювання захищеності інформації.

3. Результати навчання

Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації;

- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

- визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

- використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.

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 ресуруhttps://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. Оцінка виставляється на основі двох теоретичних модулів та трьох практичних робіт.

Модуль	Кількість балів
Основна частина	
Змістовний модуль №1	
Практична робота №1	10
Практична робота №2	10
Модульна контрольна робота № 1	40
Всього за змістовим модулем №1	60
Змістовний модуль №2	
Практична робота №3	10
Модульна контрольна робота № 2	20
Всього за змістовим модулем №2	30
Додаткова частина	
Участь у Днях студентської науки	10
Разом	100

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". http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

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.

7.6. Бонуси

За активність та правильні відповіді на лекційних та лабораторних заняттях студент може отримати до +2 балів до семестрової оцінки на кожному занятті.

8 Рекомендовані джерела інформації

Базові

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.

Додаткові

1. Богуш В.М. Інформаційнабезпекадержави / 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-правовезабезпеченняінформаційноїбезпеки / 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

. **Інформаційні ресурси**

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