


СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «КІБЕРОПЕРАЦІЇ»

	Ступінь освіти	бакалавр
	Галузь знань	12 Інформаційні технології
	Тривалість викладання	3,4 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=3105>

Кафедра, що викладає

Безпеки інформації та телекомунікацій

Інформація про викладачів



Ковальова Юлія Вікторівна	к.т.н., доцент
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/kovaleva.php
E-mail:	kovalova.yu.v@nmu.one

1. Анотація до курсу

Студенти отримують комплексні знання та практичні навички з планування, розгортання та управління кіберзахистом на рівнях індивідуального, корпоративного та національного. Це включає в себе вивчення методів проведення кібероперацій в інформаційному просторі, що відіграють важливу роль в комплексному захисті інформації на всіх рівнях.

2. Мета та завдання курсу

Мета дисципліни кібероперації полягає в поглибленому вивченні та засвоєнні студентами знань, навичок і компетенцій, необхідних для розуміння, застосування та ефективного впровадження стратегій, технологій та методів в кібербезпеці та кіберопераціях.

Завдання курсу полягає у формуванні здатності здобувачів вищої освіти обґрунтовано використовувати знання щодо впливу кібероперацій на інформаційний простір в цілому..

3. Результати навчання

- Здатність аналізувати та ідентифікувати різноманітні кіберзагрози, включаючи кібератаки, кібершпигунство, кібертероризм тощо.
- Навички розробки та впровадження ефективних стратегій кіберзахисту, які враховують специфіку потенційних загроз та вразливостей.
- Оволодіння сучасними технологіями та інструментами кібербезпеки для виявлення, запобігання та реагування на кіберзагрози.
- Розуміння етичних принципів та правових аспектів, пов'язаних з кіберопераціями та кібербезпекою.
- Підготовка студентів до реальних ситуацій та викликів, пов'язаних з кібербезпекою в сучасному інформаційному середовищі.

4. Структура курсу

ЛЕКЦІЇ

Лекція 1: Вступ до кібероперацій

- Визначення понять: кібероперації, кібербезпека, кіберзагрози.
- Історія розвитку кібероперацій.
- Важливість кібербезпеки у сучасному світі.

Лекція 2: Основи кібербезпеки

- Основні принципи захисту інформації.
- Типи кіберзагроз та їх характеристики.
- Методи захисту від кібератак.

Лекція 3: Архітектура систем кібербезпеки

- Структура та компоненти системи кібербезпеки.
- Засоби виявлення та моніторингу кіберзагроз.
- Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS).

Лекція 4: Кібервійна та кібершпигунство

- Поняття кібервійни та її особливості.
- Кібершпигунство: методи, техніки та захист.

Лекція 6: Соціальна інженерія та соціальні аспекти кібербезпеки

- Соціальна інженерія: визначення та приклади.
- Вплив соціальних мереж на кібербезпеку.
- Заходи захисту від соціальної інженерії.

Лекція 7: Законодавство та етика в кіберпросторі

- Міжнародне законодавство про кібербезпеку.
- Етичні аспекти використання кібертехнологій.
- Відповідальність за кіберзлочини.

Лекція 8: Технічні засоби кіберзахисту

- Програмне забезпечення для виявлення загроз.
- Антивірусне програмне забезпечення та файрволи.
- Захист від вразливостей та використання регулярних оновлень.

Лекція 9: Стратегії та техніки відновлення після кібератаки

- Планування відновлення після інциденту.

- Відновлення даних та систем після кібератаки.
- Уроки з кібербезпеки та попередження майбутніх інцидентів.

ПРАКТИЧНІ ЗАНЯТТЯ

1. Кібервійна та кібершпигунство

Роль кібервійни та кібершпигунства в сучасному світі.

Проведення аналізу чинників з кібервійни та виявлення кібершпигунства.

2. Етика та законність у кіберпросторі

Обговорення етичних та правових аспектів використання кібертехнологій.

3. Вирішення етичних дилем та дотримання законодавства в контексті кібероперацій.

5. Технічне обладнання та/або програмне забезпечення

Необхідний доступ до системи дистанційного навчання НТУ «ДП». Активованій 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	Вирішення практично-ситуаційних задач у сфері безпеки інформації в аспекті кібероперацій з використанням нормативно-правової бази України та міжнародного законодавства	Доступ до електронного ресурсу 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 задачі 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 (вигадкування 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 відбутись в он-лайн формі за погодженням з керівником курсу.

8 Рекомендовані джерела інформації

8.1. Основні

- "Hacking: The Art of Exploitation" by Jon Erickson
- "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto
- "Cybersecurity Essentials " by Charles J. Brooks and Christophe rGrow
- "Practical Malware Analysis: The Hands-On Guideto Dissecting Malicious Software" by Michael Sikorski and Andrew Honig

8.2. Журнали та статті:

- IEEE Security&Privacy
- Journal of Cybersecurity
- Security Focus
- Dark Reading

8.3. Веб-ресурси:

- OWASP (OpenWeb Application Security Project) - ресурс зі збору та поширення інформації про захист веб-додатків
- SANS Institute - навчальний ресурс з кібербезпеки та інформаційної безпеки
- Krebson Security - блог про кібербезпеку від журналіста Браяна Кребса
- The Hacker News - новини та аналітика зі світу кібербезпеки

8.4. Онлайн платформи:

- Coursera: "Cybersecurity Specialization" від Університету Меріленда
- edX: "Cybersecurity Micro Masters Program" від Рочестерського університету

- UdeMy: "Complete Cyber Security Course: Beginner to Advanced" від Нейла Меркела
- Документація та матеріали від провідних вендорів з кібербезпеки:
- Документація та руководства користувача від Cisco, Palo Alto Networks, Check Point, Fortinet та інших провідних виробників з кібербезпеки.

8.5. Інформаційні ресурси

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