СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «КІБЕРОПЕРАЦІЇ»

Ступінь освіти	бакалавр
Спеціальність	113 Прикладна математика 121 Інженерія програмного забезпечення 122 Комп'ютерні науки 125 Кібербезпека та захист інформації 172 Електронні комунікації та радіотехніка
Тривалість викладання	3,4 чверті
Заняття:	Весняний 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=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

Студентиотримуюткомплекснізнання та практичнінавички з планування, розгортання та управліннякіберзахистом на рівняхіндивідуального, корпоративного та національного. Цевключає в себе вивченняметодів 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 кібероперація.

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

3. Результати навчання

- Здатність аналізувати та ідентифікувати різноманітні кіберзагрози, включаючи кібератаки, кібершпигунство, кібертероризм тощо.
- Навичкирозробки та впровадженняефективнихстратегійкіберзахисту, яківрахуютьспецифікупотенційнихзагроз та вразливостей.
- Оволодіннясучаснимитехнологіями та інструментамикібербезпеки для виявлення, запобігання та реагування на кіберзагрози.
- Розумінняетичнихпринципів та правовихаспектів, пов'язаних з кібероперaціями та кібербезпекою.
- Підготовкастудентів до реальнихситуацій та викликів, пов'язаних з кібербезпекою в сучасномуінформаційномусередовищі.

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 сучасномусвіті.
Проведенняаналізу чинників з кібервійни та виявленнякібершпигунства.

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». 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	Вирішення практично-ситуаційних задач у сфері безпеки інформації в аспекті кібероперацій 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. 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

1. Michael G. Solomon, Jason Andress – "Security Strategies in Cybersecurity and Cyber Warfare: Strategic Approaches to Cybersecurity", Видавництво: Jones & Bartlett Learning, 2021, ISBN: 978-1284090636, Сторінки: 400

2. David E. Sanger – "The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age", Видавництво: Crown, 2018, ISBN: 978-0451497895, Сторінки: 384

3. Shon Harris, Fernando Maymi – "CISSP All-in-One Exam Guide", Видавництво: McGraw-Hill Education, 2018 (8-е видання), ISBN: 978-1260142655, Сторінки: 1456

4. Christopher Hadnagy – "Social Engineering: The Science of Human Hacking", Видавництво: Wiley, 2018 (2-е видання), ISBN: 978-1119433385, Сторінки: 400

5. William Stallings – "Cryptography and Network Security: Principles and Practice", Видавництво: Pearson, 2016 (7-е видання), ISBN: 978-0134444284, Сторінки: 800

6. Kimberly K. Merritt, Jason Andress – "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners", Видавництво: Syngress, 2014, ISBN: 978-0124166721, Сторінки: 324

7. Jon DiMaggio – “The Art of Cyberwarfare: An Investigator’s Guide to Espionage, Ransomware, and Organized Cybercrime”, Видавництво: No Starch Press, 2022, ISBN: 978-1718502147, Сторінки: 288

8. Andy Greenberg – “Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers”, Видавництво: Doubleday, 2019, ISBN: 978-0385544405, Сторінки: 368

9. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

10. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

11. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

12. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

13. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.

14. ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.

15. ДСТУ 1.5:2003 Правила побудови, викладання, оформлення та вимоги до змісту нормативних документів.

16. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.

17. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

18. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

19. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 04.12.2000 № 53.

20. НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці”, затверджене наказом Адміністрації Держспецзв’язку від 15.04.2013 № 215

21. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

22. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.