


СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Технології забезпечення інформаційної і кібербезпеки об'єктів»

	Ступінь освіти	магістр
	Освітня програма	Кібербезпека
	Тривалість викладання	1,2 чверті
	Заняття:	осінній семестр
	лекції:	3 години
	практичні заняття:	2 години
	Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: <https://do.nmu.org.ua/course/view.php?id=5375>

Кафедра, що викладає

Безпеки інформації та телекомунікацій

Інформація про викладачів:



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

1. Анотація до курсу

Інформаційна сфера, як системоутворюючий фактор життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових національної безпеки України.

Саме об'єкти критичної інфраструктури потребують детального вивчення та аналізу, тому що представляють стратегічне значення для країни та її національної безпеки в цілому.

Сучасний розвиток інформаційного простору зумовлює втілення нових наукових та/або прикладних досліджень у галузі інформаційної безпеки та/або кібербезпеки, що актуалізує питання захисту інформації об'єктів критичної інфраструктури.

2. Мета та завдання курсу

Мета дисципліни – формування у студентів систематизованої сукупності відомостей та вмій про інформаційну безпеку держави та шляхи її забезпечення. Мати компетентність щодо визначення місця інформаційної безпеки в загальній системі національної безпеки та вплив дестабілізуючих факторів та інформаційних загроз на безпеку особистості, суспільства та держави, основи інформаційного протиборотства та інформаційної боротьби та орієнтуватися в загальних підходах до забезпечення безпеки інформаційних технологій.

Завдання курсу:

- ознайомити здобувачів вищої освіти із основними принципами забезпечення національної безпеки;
- ознайомити здобувачів вищої освіти з основними напрямками державної політики з питань національної безпеки в інформаційній сфері;
- ознайомити здобувачів вищої освіти із методами ведення інформаційних війн та вплив соціального інжинірингу на суспільство в цілому;
- ознайомити здобувачів вищої освіти зі способами несанкціонованого зняття інформації з технічних каналів її витоку
- ознайомити здобувачів вищої освіти з основними факторами кіберзахисту об'єктів критичної інфраструктури;
- ознайомити здобувачів вищої освіти із концепцією суспільних зв'язків як системи впливу на людей у секторі кібербезпеки.

3. Результати навчання

Проводити дослідницьку діяльність в сфері інформаційної безпеки та/або кібербезпеки із використанням сучасних технологій забезпечення інформаційної і кібербезпеки об'єктів.

Застосовувати, розробляти та удосконалювати інформаційні технології, математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки на основі сучасних технологій забезпечення інформаційної і кібербезпеки об'єктів.

Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на сучасних технологій забезпечення інформаційної і кібербезпеки об'єктів.

Аналізувати та оцінювати захищеність систем та засобів кіберзахисту, технології створення та використання сучасних технологій забезпечення інформаційної і кібербезпеки об'єктів.

Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

Розробляти та використовувати сучасні технології забезпечення інформаційної і кібербезпеки об'єктів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

4. Структура курсу

ЛЕКЦІЇ

Технології забезпечення інформаційної безпеки.

1. Основні принципи забезпечення національної безпеки
2. Загрози кібербезпеці і безпеці інформаційних ресурсів
3. Національні інтереси держави в інформаційній сфері.
4. Основні напрями державної політики з питань національної безпеки в інформаційній сфері
5. Кібершпionaж як частина побудови системи безпеки
6. Технічні канали витоку інформації.
7. Способи несанкціонованого зняття інформації з технічних каналів її витоку
8. Стратегічні комунікації як вектор розвитку інформаційної безпеки
9. Основні фактори впливу методів проведення кібероперацій
10. Концепція суспільних зв'язків як системи впливу на людей у секторі безпеки

11. Заходи щодо боротьби з кіберзлочинністю

Механізми забезпечення кіберстійкості критичної інфраструктури (КІ). Побудова систем кіберзахисту КІ.

12. Методичне та організаційне забезпечення кіберзахисту КІ.

13. Ідентифікація кіберзагроз та оцінювання ризиків порушення функціонування КІ.

14. Визначення вимог до кіберзахисту об'єктів КІ.

15. Пректування систем кіберзахисту об'єктів КІ:

- Захист систем обробки та аналізу інформації;
- Захист систем управління технологічним процесом.

Взаємодія суб'єктів національної системи захисту КІ та обмін інформацією з питань безпеки і стійкості функціонування КІ.

16. Захист інформаційних систем та інформації об'єктів КІ.

Методичне та організаційне забезпечення кіберзахисту КІ.

17. Методичне та організаційне забезпечення взаємодії та обміну інформацією з питань кіберзахисту КІ.

Ідентифікація кіберзагроз та оцінювання ризиків порушення функціонування КІ.

18. Процедури та алгоритми обробки інформації з питань стану кібербезпеки КІ, оцінки ризиків та планування заходів забезпечення безпеки і стійкості КІ.

Визначення вимог до кіберзахисту об'єктів КІ.

ПРАКТИЧНІ ЗАНЯТТЯ

1. Світовий досвід побудови системи інформаційної безпеки на об'єктах стратегічного значення
2. Побудова принципів впровадження нормативних актів в систему інформаційного захисту
3. Класифікація каналів витоку інформації
4. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів її витоку
5. Методи та засоби блокування технічних каналів витоку інформації
6. Методи захисту інформації у телекомунікаційних мережах та відкритих каналах зв'язку

5. Технічне обладнання та/або програмне забезпечення

Технічні засоби навчання: мультимедійні та комп'ютерні пристрої.

Програмні засоби дистанційної освіти: MS Office 365, MS Teams, дистанційна платформа Moodle.

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		
53	42	30	5	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:

53 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.

7 балів – Достатня зрозумілість відповіді

5 бали – Добра зрозумілість відповіді

3 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". 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

Наприкінці вивчення курсу та перед початком сесії здобувача вищої освіти буде запропоновано анонімно заповнити електронні анкети (Microsoft Forms Office 365), які буде розіслано на ваші університетські поштові скриньки. Заповнення анкет є важливою складовою вашої навчальної активності, що дозволить оцінити дієвість застосованих методів викладання та врахувати ваші пропозиції стосовно покращення змісту навчальної. За участь у анкетуванні здобувач вищої освіти отримує **5 балів**.

8 Рекомендовані джерела інформації

1. Ковальова Ю.В. Технологічні аспекти побудови мереж інформаційної безпеки об'єктів критичної інфраструктури. Монографія «Innovative Technologies in the Formation and Development of Human Capital», Вища Технічна Школа, м. Катовіца, Польща, 2018. С. 27-37. ISBN: 978–83–947093–6–5.

2. Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. — К.: ІСЗЗІ КПІ ім. Ігоря Сікорського», 2018. — 297 с.
3. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. – К.: Видавництво НА СБ України, 2020. – 256 с.
4. YuliiaKovaleva, TetianaBabenko, ViraIgnisca. Models And Methods Of Wireless Decentralized Networks For Energy Monitoring Of Critical Infrastructure Facilities. Scientific and practical cybersecurity journal. Georgia. **Issue No:** 4, December, 2020. ISSN 2587-4667 <https://journal.scsa.ge/issue/december-2020/>
5. Zhang Z., Mehmood A., Shu L., Huo Z., Zhang Y., Mukherjee M. A survey on fault diagnosis in wireless sensor networks. IEEE Access, vol. 6, pp. 11349-11364, 2018.
6. Kovalova Y., Babenko T., Oksiiuk O., Myrutenko L. Optimization of Lifetime In Wireless Monitoring Networks. International Journal o Computing. Research Institute for Intelligent Computer Systems, 2020 № 19 (2), Pp. 267–272. ISSN: 2312-5381.
7. KathrynCave. TheIoT “timebomb” report: 49 security experts sharet heir views.- <http://www.idgconnect.com/abstract/12744/the-iot-bomb-report-49-security-experts-share-views>