СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Системи управління інформаційною безпекою»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**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=1368

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладачів:

Корченко Анна Олександрівна	професор, д.т.н.
Персональна сторінка	http://bit.nmu.org.ua/ua/pro_kaf/prepods/Korchenko.php
E-mail:	**korchenko.a.o@nmu.one**

Тимофєєв Дмитро Сергійович	старший викладач
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/timofeev.php
E-mail:	**tymofieiev.d.s@nmu.one**

1. Анотація до курсу

У сучасних умовах багато зроблено в напрямку забезпечення безпеки інформації, але мало що запропоновано для управління захисними заходами, які впроваджуються в організації. Часто організації не усвідомлюють, які активи є більш критичними, які ризики інформаційної безпеки пов'язані з цими активами, які захисні заходи необхідно планувати і чому. Всі ці проблеми можна вирішити при ефективному управлінні інформаційною безпекою в організації за рахунок СУІБ.

Розвиток централізованої СУІБ на організаційному рівні залежить від внутрішніх і зовнішніх факторів, які часто конфліктують. Тому вони вимагають різних комбінацій структур, процесів і механізмів, що забезпечують безпеку їх

інформаційної інфраструктури і покращують її найкращим чином, реалізуючи політику, прийняту організацією.

У даному курсі детально розглядаються фундаментальні аспекти, пов'язані зі складним процесом управління інформаційною безпекою, що складається з безлічі видів діяльності і охоплюють всю організацію незалежно від її масштабів і сфери діяльності, а також планування, впровадження, верифікації та вдосконалення СУІБ, що реалізують цей процес.

2. Мета та завдання курсу

Мета дисципліни – формування у здобувачів вищої освіти компетентностей щодо планування, впровадження, підтримки та модернізації систем управління інформаційною безпекою..

Завдання курсу:

- ознайомити здобувачів вищої освіти із основними підходами до управління інформаційною безпекою;
- ознайомити здобувачів з застосуванням основних стандартів з систем і процесів управління інформаційною безпекою;
- ознайомити здобувачів із основними вимогами та принципами, що враховуються при розробці та впровадженні політики ІБ;
- ознайомити здобувачів із особливостями ризик-орієнтованого підходу до управління інформаційною безпекою;
- ознайомити здобувачів вищої освіти з методами, засобами та заходами аудиту та моніторингу ефективності функціонування інформаційних систем і технологій у сфері інформаційної та кібербезпеки;
- ознайомити здобувачів вищої освіти з методами і заходами протидії кіберінцидентам, надавати рекомендації щодо попередження та аналізу кіберінцидентів.

3. Результати навчання

Аналізувати та оцінювати системи управління інформаційною безпекою, комплексів та засобів кіберзахисту, технології використання спеціалізованого програмного забезпечення.

Розв’язувати складні задачі професійної діяльності в галузі управління інформаційною безпекою на основі обґрунтування використання, впровадження та аналізу кращих світових стандартів, практик

Розробляти і супроводжувати системи управління інформаційної безпеки та кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою організації на базі стратегії і політики інформаційної безпеки.

Аналізувати та контролювати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки організації.

Розробляти та впроваджувати методи і заходи протидії кіберінцидентам, надавати рекомендації щодо попередження та аналізу кіберінцидентів.

Аналізувати, розробляти і супроводжувати заходи аудиту та моніторингу ефективності функціонування інформаційних систем і технологій у сфері інформаційної та\або кібербезпеки.

4. Структура курсу

ЛЕКЦІЇ **115**

1 Характеристика та обрання основних підходів до управління інформаційною безпекою

1. Базова термінологія
1.1. Система
1.2. Системний підхід
1.3. Процес
1.4. Процесний підхід
1.5. Управління
1.6. Циклічна модель поліпшення процесів
1.7. Системний підхід до управління організацією
1.8. Процесний підхід до управління організацією
1.9. Інформаційна безпека

2 Аналіз та застосування основних стандартів з систем і процесів управління інформаційною безпекою

2. Стандартизація систем і процесів управління інформаційною безпекою
2.1. Серія стандартів ISO / IEC 27000 «Інформаційні технології. Методи забезпечення безпеки »
2.1.1. ISO / IEC 27000- СУІБ: визначення та основні принципи
2.1.2. ISO / IEC 27001 вимоги до СУІБ
2.1.3. ISO / IEC 27002 практичні правила управління ІБ
2.1.4. ISO / IEC 27003 посібник з впровадження СУІБ
2.1.5. ISO / IEC 27004 оцінка функціонування СУІБ
2.1.6. ISO / IEC 27005 управління ризиками ІБ
2.1.9. ISO / IEC 27011 посібник з управління ІБ для телекомунікаційних компаній на основі ISO / IEC 27002
2.1.10. ISO / IEC 27013 - керівництво з інтегрованого впровадження стандартів ISO / IEC 20000 і 27001
2.1.11. ISO / IEC 27014 - інфраструктура керівництва ІБ
2.1.12. ISO / IEC 27015 - керівництво з управління ІБ для фінансових сервісів
2.1.13. ISO / IEC 27031 - керівництво по готовності інформаційних і телекомунікаційних технологій для забезпечення безперервності бізнесу
2.1.14. ISO / IEC 27033 - управління безпекою мереж
2.1.15. ISO / IEC 27035-управління інцидентами ІБ
2.1.16. ISO / IEC 27037- керівництво по ідентифікації, збору та / або отриманню і забезпеченню збереження свідчень, представлених в електронній формі
2.2. Стандарти на окремі процеси управління ІБ і оцінку безпеки ІТ
2.2.1. ISO / IEC 13335 - методи і засоби забезпечення безпеки інформаційних

технологій
2.2.2. ISO / IEC 15408 та ISO / IEC 18045 - загальні критерії та методології оцінки безпеки інформаційних технологій

3 Розробка та аналіз політики інформаційної безпеки

3. Політика інформаційної безпеки
3.1. Поняття політики забезпечення ІБ і політики ІБ організації
3.2. Причини розробки політики ІБ
3.3. Основні вимоги та принципи, що враховуються
при розробці та впровадженні політики ІБ
3.4. Зміст політики ІБ
3.4.1. Зміст корпоративної політики ІБ
3.4.2. Зміст приватних політик ІБ
3.5. Життєвий цикл політики ІБ
3.5.1. Розробка політики ІБ
3.5.2. Впровадження політики ІБ
3.5.3. Застосування політики ІБ
3.5.4. Анулювання політики ІБ
3.6. Відповідальність за виконання політики ІБ

4 Запровадження управління ІБ із застосуванням СУІБ

4. Управління і система управління інформаційною безпекою
4.1. Необхідність управління забезпеченням ІБ організації
4.2. Діяльність по забезпеченню ІБ організації як процес
4.3. Визначення управління ІБ організації
4.4. Управління ІБ інформаційно-телекомунікаційних технологій організації
4.5. Система управління ІБ організації
4.5.1. Область дії СУІБ
4.5.2. Документальне забезпечення СУІБ
4.5.3. Політика СУІБ
4.5.4. Підтримка СУІБ з боку керівництва

ПРАКТИЧНІ ЗАНЯТТЯ 65

1. Дослідження реальних об’єктів інформаційної діяльності
2. Розробка проекту реалізації СУІБ
3. Інвентаризація та класифікація інформаційних активів
4. Програмне моделювання процесу управління ризиками інформаційної безпеки
5. Розробка політики безпеки інформації

РАЗОМ 180

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		
55	40	30	5	**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.

8 балів – Достатня зрозумілість відповіді

6 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 дисципліни. За участь у анкетуванні здобувач вищої освіти отримує **5 балів**.

8 Рекомендовані джерела інформації

1.Шелест, М.Є., Корченко, О.Г., Іванченко, Є.В., Ткач, Ю.М. , Казмірчук, С.В. Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125" Кібербезпека".Ніжин : ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.

2. Закон України Про захист інформації в інформаційно-телекомунікаційних системах № 80/94-ВР від 05.07.1994 р., [Електронний ресурс]. – Режим доступу :https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

3. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.

4. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

5. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

6. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

7. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT)