МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

м. Кропивницький

1. Загальна інформація

Назва дисципліни	Менеджмент інформаційної безпеки
Викладач	Лисенко Ірина Анатоліївна, кандидат технічних наук, старший викладач кафедри кібербезпеки та програмного забезпечення http://kbpz.kntu.kr.ua/lysenko-irina/ https://scholar.google.com.ua/citations?user=b5TXV7EAAAAJ&hl=ru&authuser=2 https://orcid.org/0000-0003-4394-4960
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8^{30} до 14^{20} Мобільні телефони / Viber / Telegram надано у описі курсу «Спеціальні розділи математики для кібербезпеки» на сервері дистанційної освіти ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=650
E-mail:	lisenkoia@kntu.kr.ua
Консультації	*Очні консультації* згідно до затвердженого розкладу консультацій. *Онлайн консультації* засобами електронної пошти, мессенджерів (Facebook-Messenger / Viber / Telegram) у робочі дні

2. Анотація до дисципліни

Дисципліна «Менеджмент інформаційної безпеки» належить до вибіркових навчальних дисциплін забезпечення навчального процесу за освітнім ступенем «Бакалавр».

Даний курс знайомить студентів із основними питаннями менеджменту інформаційної безпеки, зокрема впровадженням політики інформаційної безпеки; організації інформаційної безпеки, її внутрішньої організації, політику щодо мобільного обладнання та віддаленої роботи; заходами управління ресурсами СУІБ: відповідальності за ресурси СУІБ, класифікації інформації та поводження з носіями; криптографічних засобів захисту, політикою використання криптографічних засобів; заходами фізичної безпеки та безпеки інфраструктури: зони безпеки, обладнання; засобами забезпечення безпеки експлуатації, зокрема безпечні процедури експлуатації та відповідальності, захисту від зловмисного коду, резервне копіювання, ведення журналів аудиту та моніторинг, управління технічною вразливістю, розгляд аудиту інформаційних систем; засобами забезпечення безпеки експлуатації; засобами забезпечення безпеки комунікацій; засобами забезпечення вимог щодо відносин з постачальниками: інформаційна безпека у взаємовідносинах з постачальниками, управління наданням послуг постачальником.

Мета і завдання дисципліни

Мета: Метою вивчення курсу «Менеджмент інформаційної безпеки» є формування комплексу знань щодо основ менеджменту інформаційної безпеки, набуття студентом теоретичних знань та практичних навичок щодо управління інформаційною безпекою в інформаційно-телекомунікаційних (автоматизованих) системах для реалізації встановленої політики безпеки.

Основними **завданнями** вивчення дисципліни є формування наступних компетенцій:

Здатність застосовувати знання у практичних ситуаціях.

Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою

здійснення професійної діяльності.
Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно- правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням електронних презентацій, поєднуючи із лабораторними заняттями.

Формат очний (offline / Face to face)

Для заочної форми

Під час сесії формат очний (Face to face), у міжсесійний період – дистанційний(online).

5. Результати навчання

Програмні результати вивчення дисципліни:

Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

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

Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та кібербезпеки;

Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації

Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та або кібербезпеки для розслідування інцидентів.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Кількість годин
Кількість кредитів/годин	4/120
Кількість змістових модулів	2
Нормативна/вибіркова	вибіркова
Вид підсумкового контролю: залік	-

7. Технічне й програмне забезпечення/обладнання

Лекційні заняття проводяться в аудиторіях обладнаних мультимедійним проектором. Практичні роботи виконуються у аудиторіях кафедри кібербезпеки та програмного забезпечення, обладнаних відповідним апаратним та програмним забезпеченням (ауд 501, 507, 508, 517). Оскільки при вивченні дисципліни використовуються інформаційні технології навчання, система дистанційної освіти Moodle, бажано мати комп'ютерну техніку (з виходом у глобальну мережу) для виконання тестових завдань в системі дистанційної освіти та підготовки (друку) рефератів і самостійних робіт.

Програмне забезпечення	Вільне ПЗ чи ні	Матеріально-технічне забезпечення
		Лекційні заняття проводяться у ауд. 500 обладнаною мультимедійним проектором Epson EB-X41. Лабораторні роботи виконуються у лабораторіях кафедри кібербезпеки та програмного забезпечення, (ауд 501, 505, 507, 508, 517), з відкритою бездротовою мережею Wi-Fi, вільним доступом до Інтернету.
GoogleChrome https://play.google.com/store/apps/details?id=com.android.chrome&hl=uk&gl=U	вільне	

8. Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення.
Детальніше за посиланням URL : http://www.kntu.kr.ua/doc/dobro.pdf

Відвідування занять

Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і практичні заняття курсу.
Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ; Кодексу академічної доброчесності ЦНТУ.

9. Програма навчальної дисципліни

Тема 1 - Передумови й основні напрямки розвитку менеджменту в галузі інформаційної безпеки
Тема 2 - Діяльність міжнародних організацій у галузі інформаційної безпеки
Тема 3 - Діяльність спеціалізованих міжнародних організацій і об'єднань у галузі інформаційної безпеки
Тема 4 - Управління інформаційною безпекою на рівні великих постачальників інформаційних систем.
Тема 5. Управління інформаційною безпекою на державному рівні: загальні принципи і практика України
Тема 6. Організаційне забезпечення інформаційної безпеки на державному рівні: практика США
Тема 7. Менеджмент інформаційної безпеки на рівні підприємства: основні напрямки і структура політики безпеки
Тема 8. Склад деталізованої політики безпеки
Тема 9. Департамент інформаційної безпеки і робота з персоналом
Тема 10. Організація реагування на надзвичайні ситуації (інциденти)
Тема 11. Аудит стану інформаційної безпеки на підприємстві
Тема 12. Програмні засоби, що підтримують управління інформаційною безпекою на підприємстві
Тема 13. Надання послуг в сфері інформаційної безпеки
Тема 14. Економіка інформаційної безпеки

10. Система оцінювання та вимоги

Методи контролю: спостереження за навчальною діяльністю студентів, усне опитування, письмовий контроль, тестовий контроль.
Форма підсумкового контролю: залік.

Контроль знань і умінь (поточний і підсумковий) з дисципліни «Менеджмент інформаційної безпеки» здійснюється згідно з кредитною трансфернонакопичувальною системою організації навчального процесу. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою.

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, практичні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті:

Підсумкова (загальна оцінка) курсу навчальної дисципліни є сумою рейтингових оцінок (балів), одержаних за окремі оцінювані форми навчальної діяльності: поточне та підсумкове тестування рівня засвоєності теоретичного матеріалу під час аудиторних занять та самостійної роботи (модульний контроль); оцінка (бали) за виконання практичних індивідуальних завдань. Підсумкова оцінка виставляється після повного вивчення навчальної дисципліни, яка виводиться як сума проміжних оцінок за змістові модулі.

11. Рекомендована література

Базова

1. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. –Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с. : іл.
2. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука – Харків: 2018. – 289 с. [Електронний ресурс]. – Режим доступу: https://cutt.ly/5ugjj6s
3. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с
4. Зубок М.І. Інформаційна безпека в підприємницькій діяльності / М.І. Зубок. – К.: ГНОЗІС, 2015 - 216 с.

Допоміжна

1. Моделювання економічної безпеки: держава, регіон, підприємство :[монографія] / [Геєць В. М., Кизим М. О., Клебанова Т. С., Черняк О. І. та ін.] ; за ред. Гейця В. М. – Х. : ВД "ІНЖЕК", 2006. – 240 с
2. Мунтіян В. І. Економічна безпека України : [підруч.] / В. І. Мунтіян. – К. :КВІСТ, 1999. – 457 с.
3. Аристотель. Політика / Пер. з давньогр. та передм. О. Кислюка. Київ: Основа, 2000. 239 с.
4. Василенко В. Збройна агресія Росії проти України: геополітичний та національний виміри // Юридичний вісник України.№ 42 (1007). 18–24 жовтня 2014. С. 6–7.

Інформаційні ресурси

1. ДСТУ ISO 15408-1: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 1. Вступ і загальна модель.
2. ДСТУ ISO 15408-2: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 2. Функціональні вимоги безпеки.
3. ДСТУ ISO 15408-3: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 3. Вимоги до забезпечення захисту.
4. ДСТУ ISO 17799: 2005. Інформаційні технології. Методи захисту. Практичні рекомендації з управління інформаційної безпеки.

5. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : Підручник [Електронний ресурс] / [В.Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа], заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с. – Режим доступу: http://www.dut.edu.ua/uploads/p_303_79299367.pdf .
6. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [КорченкоО.Г., Гнатюк С.О., КазмірчукС.В. та ін.]. –К.: Центр навч.-наук. та наук.-пр.видань НАСБ України, 2014. – 190 с. – Режим доступу: http://193.178.34.24/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf.