Силабус навчальної дисципліни
«*МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ*»

Спеціальність	*125 Кібербезпека*
Освітня програма	*Кібербезпека*
Освітній рівень	*Бакалавр*
Статус дисципліни	*Базова*
Мова викладання	*Українська*
Курс / семестр	*2 курс., 4 семестр*
Кількість кредитів ЄКТС	*4*
Розподіл за видами занять та годинами навчання	*Лекції – 24 год.*
	Практичні (семінарські) – 0 год.
	Лабораторні – 24 год.
	Самостійна робота – 72 год.
Форма підсумкового контролю	*залік*
Кафедра	*Кібербезпеки та інформаційних технологій, м. Харків, пр-т Науки 9-А, 057-702-18-31, http://www.kafcbit.hneu.edu.ua/*
Викладач (-і)	*Мілевський Станіслав Валерійович, к.е.н., доцент*
Контактна інформація викладача (-ів)	*Stanislav.Milevskiy@hneu.net*
Дні занять	*http://www.kafcbit.hneu.edu.ua/teachers/*
Консультації	*Розклад занять: http://services.hneu.edu.ua:8081/schedule/selection.jsf*

Метою навчальної дисципліни “Менеджмент інформаційної безпеки” є формування теоретичних знань основних принципів менеджменту управління інцидентами та ризиками на основі вимог міжнародних регуляторів.

Передумови для навчання
Інформаційна безпека держави
Основи побудови та захисту сучасних операційних систем
Введення в мережі

Зміст навчальної дисципліни

Змістовий модуль 1. Ефективне управління інцидентами інформаційної безпеки за вимогами міжнародних стандартів

Тема 1. Теоретичні основи менеджменту інформаційної безпеки

Тема 2. Модель PDCA опису життєвого циклу процесів управління інцидентами інформаційної безпеки. Етапи ефективного менеджменту інцидентів інформаційної безпеки за вимогами міжнародних стандартів ISO 27035 та ISO 18044

Тема 3. Особливості менеджменту інцидентів за вимогами міжнародного стандарту ITIL. Концепція побудови, структура та функціональні особливості ефективної системи менеджменту інцидентів ІБ

Тема 4. Поняття групи реагування на інциденти ІБ (CERT / CSIRT): історія розвитку та можливі вигоди перед- прийняттю. Узагальнена класифікація груп CERT / CSIRT: сфера діяльності, цілі та потенційні клієнти

Тема 5. Базові етапи створення груп CERT / CSIRT: від визначення середовища існування до співпраці на міжнародному рівні

Тема 6. Інструментарій для ефективного функціонування груп реагування на інциденти ІБ. Документаційне забезпечення процесу управління інцидентами ІБ. Діяльність різних груп реагування на інциденти ІБ.

Змістовий модуль 2. Ризик-менеджмент інформаційної безпеки
Тема 7. Аналіз ризиків в області захисту інформації
Тема 8. Управління ризиками та міжнародні стандарти
Тема 9. Технології аналізу ризиків
Тема 10. Інструментальні засоби аналізу ризиків
Тема 11. Аудит безпеки і аналіз ризиків
Тема 12. Виявлення атак і управління ризиками

Матеріально-технічне (програмне) забезпечення дисципліни

Internet, MS Office

Сторінка курсу на платформі Moodle (персональна навчальна система) Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною Менеджмент інформаційної безпеки https://pns.hneu.edu.ua/course/view.php?id=4924..	*Посилання:*

Рекомендовані джерела

Основна

1. Р. В. Грищук, та Ю. Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.

2. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. – М. : Академия АйТи : ДМК Пресс, 2008. – 384 с.

3. О. Г. Корченко, О. Є. Архипов, та Ю. О. Дрейс, "Оцінювання шкоди національній безпеці України у разі витоку державної таємниці", монографія, К: наук.-вид.центр НА СБУ України, 2014.

4. 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 .

Додаткова

5. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

6. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів національного банку України/ [Електронний ресурс]. Доступно: zakon.rada.gov.ua/laws/show/v0365500-11.

7. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Электронный ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11423.

8. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Электронный ресурс]. Доступно: http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii. Дата звернення: Груд. 7.2017.

9. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Электронный ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11425.

10. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту. [Электронный ресурс]. Доступно: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005

11. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Электронный ресурс]. доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11427.

Інформаційні ресурси.

12. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни "Менеджмент інформаційної безпеки" https://pns.hneu.edu.ua/course/view.php?id=4924.

Система оцінювання результатів навчання

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Більш детальна інформація щодо оцінювання наведена в технологічній карті дисципліни.

Накопичування рейтингових балів з навчальної дисципліни *(приклад)*

Види навчальної роботи	**Мах кількість балів**
Виконання практичних завдань	**10**
Захист практичних робіт	**50**
Поточні КР	**40**
Максимальна кількість балів	**100**

Відповідність шкали оцінювання ЄКТС національній системі оцінювання та ХНЕУ ім. С. Кузнеця

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену (іспиту), диференційованого заліку, курсового проекту (роботи), практики, тренінгу	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

Політики навчальної дисципліни

Політика дотримання академічної доброчесності,
Політика щодо пропусків занять,
Політика щодо виконання завдань пізніше встановленого терміну,
тощо

Більш детальну інформацію щодо компетентностей, результатів навчання, методів навчання, форм оцінювання, самостійної роботи наведено у Робочій програмі навчальної дисципліни «Менеджмент інформаційної безпеки», 2020.

Силабус затверджено на засіданні кафедри «31» серпня 2020 р. Протокол № 2