Силабус курсу

УПАРВЛІННЯ ІНФОРМАЦІЙНО БЕЗПЕКОЮ

Ступінь вищої освіти – бакалавр
Рік навчання: 3**,**
Семестр: 2
Кількість кредитів: 4,
Мова викладання: українська

Керівник курсу

ПІП	Аліна Давлетова
Контактна інформація	a.davletova@wunu.edu.ua

Опис дисципліни

Курс «Управління інформаційною безпекою» орієнтований на формування компетентностей та умінь щодо основних підходів захисту інформації, концептуальної моделі інформаційної безпеки, розроблення, впровадження та експлуатації систем управляння інформації на об'єктах інформаційної діяльності, формування навичок аналізу систем забезпечення інформаційної безпеки з метою впровадження найкращих практик захисту інформації.. Вивчення курсу вимагає цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи та виконання індивідуальних завдань. Метою курсу є формування комплексу знань щодо підходів до визначення джерел загроз та об'єктів захисту, методів та механізмів захисту інформаційних ресурсів, нормативно-методичної бази в галузі захисту інформації, набуття студентом теоретичних знань та практичних навичок щодо управління інформаційною безпекою в інформаційно-телекомунікаційних (автоматизованих) системах для реалізації встановленої політики безпеки..

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/2	Інформаційні ресурси, що підлягають захисту.	Володіти поняттями інформаційних ресурсів, що підлягають захисту, знання сфер розповсюдження державної таємниці на інформацію, комерційної таємниці, персональних даних.	Ситуаційне опитування, тестування
2/2	Загрози безпеці інформації.	Розуміти основні поняття, здатність визначати загрози доступності, цілісності, конфіденційності інформації та вміння класифікації загроз.	Поточне опитування, тестування
2/2	Характеристики захищеності інформаційних ресурсів. Модель CIA.	Знати характеристики основних видів безпеки, рівнів безпеки. Розуміти принципи забезпечення безпеки в інформаційній сфері. Вміти застосовувати модель CIA для вирішення задач забезпечення цілісності доступності, конфіденційності.	Поточне опитування, тестування
2/2	Політика інформаційної безпеки.	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та	Усне опитування

		технічних засобів і методів, процедур, практичних прийомів та ін.).	
2/2	Соціотехнічна безпека.	Володіти поняттям соціотехнічної системи та її властивостей., методів соціального інжинірингу. Знання основних алгоритмів соціотехнічних атак на інформаційні ресурси, етапів проведення. Вміти здійснювати захист інформації від соціотехнічних атак.	Діалог, тестуваня
2/2	Національна безпека.	Розуміти поняття основних категорії теорії національної безпеки. Знати принципи та основні засоби забезпечення національної безпеки.	Поточне опитування
2/2	Кіберзлочинність.	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	Ситуаційне опитування
2/2	Інформаційне протиборство.	Володіти основними поняттями. Розуміти концепцію інформаційної війни. Знати форми інформаційної війни на державному рівні. Здатність визначати інформаційну зброю та розробляти стратегію захисту інформаційних систем.	Діалог, тестуваня
2/2	Управління ризиками інформаційної безпеки.	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	Поточне опитування
2/2	Реагування на інциденти інформаційної безпеки.	Розуміння процесу реагування на інциденти. Вміти ідентифікувати та вирішувати інциденти, планувати реагування. Здатність проводити оцінку та аналіз інцидентів.	Поточне опитування, тестування
2/4	Управління наслідками інцидентів інформаційної безпеки.	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Вміння стримування інциденту, пом'якшення та ліквідації наслідків інциденту. Володіти інструментами обробки інцидентів.	Ситуаційне опитування, тестування
2/4	Розслідування інцидентів інформаційної безпеки.	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	Поточне опитування

Літературні джерела

1. Шумейко О.О. Інформаційна безпека. Дніпровський державний технічний університет, 2019. - 155 с.
2. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
3. Мужанова Т.М. Інформаційна безпека держави. Київ: Державний університет телекомунікацій, 2019. - 131 с.
4. Bender David. Bender on Privacy and Data Protection. LexisNexis, 2020. - 2940 p.
5. Schreider Tari. Building an Effective Security Program. 2nd Edition. - Rothstein Associates Inc., 2020. - 406 p.
6. Alassouli Hidaia. Common Windows, Linux and Web Server Systems Hacking

Techniques. Independently published, 2021. - 181 p.
7. Barnum Todd. The Cybersecurity Manager's Guide: The Art of Building Your Security Program. O'Reilly Media, Inc., 2021. - 168 p.
8. Daimi K., Peoples C. Advances in Cybersecurity Management. Springer, 2021.- 497 p.
9. Alexandrou Alex. Cybercrime and Information Technology: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices. CRC Press, 2022. - 455 p.
10. Goyal D., Balamurugan S., Senthilnathan K., Annapoorani I., Israr M. (Eds.) Cyber-Physical Systems and Industry 4.0: Practical Applications and Security Management. Apple Academic Press Inc., CRC Press, 2022. - 290 p.

Політика оцінювання

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КПІЗ)	Заліковий модуль 4 (письмовий екзамен)
20 %	20 %	20 %	40 %
1. Усне опитування на заняттях (теми 1-8) - max 16 балів. 2. Письмова робота - max 42 бали. 3. Практичне завдання - max 42 бали	1. Усне опитування на заняттях (теми 9-12)- max 16 балів. 2. Письмова робота - max 44 бали. 3. Практичне завдання - max 40 бали	1. Виконання КПІЗ - max 40 балів. 2. Захист КПІЗ -max 40 балів. 3. Участь у тренінгах - max 20 балів	1. Теоретичні питання: 3 питання по 20 балів - max 60 балів. 2. Практичне завдання - max 40 балів

Шкала оцінювання:

За шкалою університуту	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістюповторного складання)
1-34		F (незадовільно з обов'язковимповторним курсом)