ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп'ютерної інженерії та інформаційних технологій

СИЛАБУС

Базова інформація про дисципліну	
Назва дисципліни	Основи інформаційної безпеки
Рівень вищої освіти / фахової передвищої освіти	Фахова передвища освіта
Семестр	І семестр
Кафедра/циклова комісія	Кафедра комп'ютерної інженерії та інформаційних технологій
Анотація курсу	Навчальна дисципліна спрямована на формування уявлення про інформаційну безпеку (ІБ); спеціалізовані заходи у сферах інформаційної та комп'ютерної безпеки; методи та засоби, що забезпечують захист сучасних інформаційних систем у професійній діяльності, пов'язаної з отриманням, обробкою, накопиченням і захистом інформації.
Сторінка курсу в MOODLE	http://78.137.2.119:1919/m72/course/view.php?id=439
Мова викладання	українська
Лектор курсу	Захарова Марія В'ячеславівна, к.т.н., доцент Канали комунікації: СДН «Moodle»: повідомлення в чаті E-mail: lecturer2020student@gmail.com
Місце дисципліни в освітній програмі	
Перелік загальних компетентностей (ЗК)	Здатність вчитися і оволодівати сучасними знаннями. Знання та розуміння предметної області та розуміння професійної діяльності. Здатність застосовувати знання у практичних ситуаціях. Здатність працювати з інформацією, у тому числі у глобальних комп'ютерних мережах.
Перелік спеціальних компетентностей (СК)	Здатність забезпечувати захист інформації в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки. Здатність системно адмініструвати, використовувати,

	адаптувати та експлуатувати наявні інформаційні технології та системи. Здатність оформляти отримані робочі результати у вигляді презентацій, науковотехнічних звітів.
Перелік програмних результатів навчання	Вміти застосовувати знання для формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації апаратних та програмних засобів комп'ютерної інженерії для вирішення технічних задач у професійній діяльності.
Опис дисципліни	
Структура навантаження на студента	Загальна кількість годин – 180 Кількість кредитів – 6 Кількість лекційних годин – 0 Кількість практичних занять – 60 Кількість годин для самостійної роботи студентів – 120 Форма підсумкового контролю – залік
Методи навчання	Словесні (інформаційна, самостійна робота з джерелами інформації, науково-популярна розповідь); Наочні (презентаційні повідомлення) Практичні (лабораторні роботи); Інтерактивні методи (дистанційні консультації).
Зміст дисципліни	
Тема 1. Основні питання та визначення інформаційної безпеки	Загальні поняття щодо інформаційної безпеки. Інформаційна безпека держави. Підхід до проблем інформаційної безпеки. Політика у сфері інформаційної безпеки.
Тема 2. Основні загрози безпеки інформації	Поняття загрози безпеки, атаки. Основні види загроз безпеки. Класифікація за метою, принципом впливу, за характером та способом впливу, за діями порушника та інші. Поняття інформаційного ресурсу. Види інформації, що підлягають захисту.
Тема 3. Джерела загроз безпеки.	Основні джерела загроз. Вплив загроз на інформаційні ресурси системи. Механізми реалізації загроз безпеки.

	Вірусні руйнівні впливи. Класифікація порушників безпеки. Модель порушника.
Тема 4. Забезпечення інформаційної безпеки об'єктів захисту.	Поняття об'єкту захисту. Механізми забезпечення безпеки, рівні захисту. Ефективна аутентифікація. Контроль доступу до мережі. Сертифікація.
Тема 5. Стандарти по забезпеченню інформаційної безпеки.	Характеристика ефективних стандартів безпеки. Міжнародні стандарти інформаційної безпеки (ІБ).
Тема 6. Визначення вразливих місць комп'ютера.	Вразливості. Методи та засоби виявлення вразливостей. Мережевий захист ПК. Методи та засоби підвищення захищеності ПК.
Тема 7. Методи та засоби забезпечення безпеки інформації.	Принципи інженерно-технічної безпеки. Використання технічних засобів захисту. Програмні засобі безпеки. Захист комп'ютерних систем.
Тема 8. Комплексний захист інформації, його задачі.	Необхідність комплексного забезпечення інформаційної безпеки (ЗІБ) Задачі комплексного ЗБІ.
Тема 9. Стратегії комплексного ЗБІ.	Характеристика стратегій ЗБІ. Етапи побудови комплексного ЗБІ стосовно стратегій безпеки. Цінні ресурси. Критерії цінності ресурсів.
Тема 10. Розробка політики безпеки.	Політика безпеки інформації, її види. Типові задачі та засоби реалізації політики ЗБІ. Якісний і кількісний аналіз ЗБІ.
Тема 11. Аудит інформаційної безпеки.	Поняття аудиту ІБ. Основні етапи проведення аудиту безпеки. Вибір критеріїв проведення аудиту.
Тема 12. Аналіз ризиків інформаційної безпеки.	Поняття ризику ІБ, характеристика, види. Методи та засоби оцінювання можливого збитку. Використання спеціалізованих інструментаріїв для оцінювання ефективності системи інформаційної безпеки.
Політика дисципліни	

Політика відвідування	Регулярне відвідування всіх видів занять, своєчасність виконання самостійної роботи. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання зорганізується в он-лайн формі за погодженням із керівником курсу.
Політика щодо дедлайнів та перескладання	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.
Академічна доброчесність	У випадку недотримання політики академічної доброчесності (плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво) передбачено повторне проходження оцінювання.

Система оцінювання

Поточний контроль здійснюється протягом семестру під час проведення практичних, семінарських та інших видів занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що дозволяє студенту отримати атестацію з предмету – 60 балів); підсумковий/ семестровий контроль, проводиться у формі заліку або іспиту, відповідно до графіку навчального процесу.
Підсумкова оцінка за умови заліку виставляється як загальна сума балів, набраних за результатами поточного контролю.

Накопичування рейтингових балів з навчальної дисципліни (залік)

Види навчальної роботи	**Мах кількість балів**
Виконання практичних робіт № 1-10 по 3 бали	30
Виконання практичних робіт № 11, 12 по 10 балів	20
Модульні контрольні роботи (2 к.р.)	20
Презентація	15
Індивідуальні практичні завдання	15
Разом	100

Шкала оцінювання

ECTS	**Бали**	**Зміст**
A	90-100	Бездоганна підготовка в широкому контексті
B	80-89	Повні знання, міцні вміння
C	70-79	Хороші знання та вміння
D	65-69	Задовільні знання, стереотипні

		вміння
E	60-64	Виконання мінімальних вимог діяльності в стандартних умовах
FX	35-59	Слабкі знання, відсутність умінь
F	1-34	Необхідний повторний курс

Список рекомендованих джерел

1. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с.
2. Інформаційна безпека держави : підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.] ; в 2 т. – Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2016. – 264 с.
3. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В.П. Горбулін, О.Г. Додонов , Д.В. Ланде. – К. : Інтертехнологія, 2009. –164 с.
4. Корченко О.Г. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія / Олександр Григорович Корченко, Олександр Євгенович Архипов, Юрій Олександрович Дрейс, Нац. акад. Служби безпеки України.– К. : Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014.– 331 с.
5. Матвієнко М. П., Розен В. П., Закладний О. М. Архітектура комп’ютера. Навчальний посібник. — К: Видавництво Ліра-К, 2016. — 264 с.
6. Мюллер Скотт. Модернизация и ремонт ПК, 19-е издание.: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2017. – 1072 с
7. Надійність, контроль комп’ютерних систем та мереж [Текст]: конспект лекцій для студентів спеціальності 123 – «Комп’ютерна інженерія » денної та заочної форм навчання / уклад. О.І. Міскевич, К.Я.Бортник. – Луцьк: Луцький НТУ, 2017. – 44 с.
8. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД “Гельветика”, 2017. – 168 с.
9. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. Відомості Верховної Ради. 2018. № 31. Ст. 241
10. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96/2016// Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899.
11. Федун І. В. Основи теорії надійності та контролю якості виробів електронної техніки: Лабораторний практикум. – Вінниця: ВДТУ,
    2003. – 71 с.

12. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року № 392/2020 «Про Стратегію національної безпеки України». [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.
13. Abhijit Gupta, Subarna Shakya, "Information System Audit; A study for security and Challenges in Nepal", in, International Journal of Computer Science and Information Security, Vol.13, No. 11 (Nov 2015) pp 1-4. Journal ISSN 1947-5500
14. Karabacak, Bilge, Sevgi Ozkan Yildirim, and Nazife Baykal. "Regulatory approaches for cyber security of critical infrastructures: The case of Turkey." Computer Law & Securi.ty Review 32, no. 3 (2016): 526-539.