ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

СИЛАБУС

Базова інформація про дисципліну	
Назва дисципліни	**СЕ134 / Комп'ютерні віруси та засоби боротьби з ними (Computer Viruses and Means of Dealing with them)**
Рівень вищої освіти / фахової передвищої освіти	Початковий рівень (короткий цикл) вищої освіти
Семестр	1
Факультет /відділення	Бакалаврської підготовки
Анотація курсу	Метою вивчення дисципліни «Комп'ютерні віруси та засоби боротьби з ними» є ознайомлення з основними поняттями про комп'ютерні віруси, історією їх виникнення, основними принципами функціонування та поширення, класифікацією та набуття необхідних знань і навичок щодо захисту інформаційних ресурсів від вірусів. Під час вивчення дисципліни студенти оволодіють знаннями щодо основних принципів й правил побудови, класифікацію, способи розповсюдження та структури комп'ютерних вірусів, класифікацію загроз безпеці комп'ютерних систем, а також, методи боротьби з ними. Навчаться застосовувати теоретичні засади й принципи побудови сучасних і перспективних електронних обчислювальних машин, локальних, корпоративних, глобальних комп'ютерних мереж, при вирішенні питань щодо захисту вказаних систем від вірусів; демонструвати розуміння сучасних проблем комп'ютерної вірусології, опанування певних прийомів низькорівневого програмування для детальнішого засвоєння властивостей та характеристик основних об'єктів файлової системи; визначати критерії ефективності використання комп'ютерних антивірусних програмних засобів для створення умов безпеки інформації; використовувати методи аналізу

	для розробки методів захисту інформації; розробляти пропозиції (проекти) з питань захисту інформації та комп'ютерних систем від вірусів; здійснювати прогнози з питань розробки та використання обчислювальної техніки, мереж, програмного забезпечення від можливих вірусних атак; оцінювати можливі наслідки застосування елементів обчислювальної техніки, програмного забезпечення та їх систем під час вірусних атак; застосовувати у власній професійній діяльності набуті знання та навички. Отримають знання з оволодіння системним аналізом методів розпізнавання комп'ютерних вірусів і їх впливом на обчислювально-керуючі комплекси підприємств, фірм, методів їх роботи й взаємодії з обчислювальним середовищем, використання системи інструментів для боротьби з ними, створенням систем захисту від вірусних атак.
Сторінка курсу в MOODLE	http://78.137.2.119:2929/course/view.php?id=674
Мова викладання	Українська
Викладач курсу	Викладач Бреус Р.В. канали комунікації: СДН «Moodle»: повідомлення в чаті. E-mail: breus.roksolana@gmail.com
Місце дисципліни в освітній програмі	
Перелік загальних компетентностей (ЗК)	Здатність до абстрактного мислення, аналізу і синтезу. Здатність вчитися і оволодівати сучасними знаннями. Здатність застосовувати знання у практичних ситуаціях. Навички використання інформаційно-комунікаційних технологій в освітньому процесі, здатність реалізувати пошук, оброблення та аналіз інформації з різних джерел
Перелік спеціальних компетентностей (СК)	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки. Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій.

Перелік програмних результатів навчання	Знати новітні технології в галузі комп'ютерної інженерії. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.
Опис дисципліни	
Структура навантаження на студента	Загальна кількість годин – 180 Кількість кредитів – 6 Кількість лекційних годин – 30 Кількість практичних годин – 30 Кількість годин для самостійної роботи студентів – 120 Форма підсумкового контролю – залік.
Методи навчання	Словесні (лекції, пояснення), наочні (демонстрація матеріалів), інструктивний, репродуктивний, частково-пошуковий, тренувальний, пояснювально-демонстраційний, проблемно-орієнтоване навчання.
Зміст дисципліни	
Тема 1. Загальні поняття про комп'ютерні віруси, історія їх виникнення та розвитку	Феномен комп'ютерних вірусів. Передісторія їх виникнення та хронологія появи вірусів. Перші випадки масового зараження комп'ютерними вірусами. Етичні проблеми пов'язані з розповсюдженням комп'ютерних вірусів. Автори вірусів. Умови первинного зараження комп'ютера вірусом. Умови неможливості зараження комп'ютера вірусом.
Тема 2. Основні принципи функціонування комп'ютерних вірусів.	Ознаки присутності вірусних програм. Загальні принципи функ- ціонування комп'ютерних вірусів, їх розмноження. Структура ("ана- томія") комп'ютерного вірусу. Деструктивні можливості вірусів.

Тема 3. Класифікація комп'ютерних вірусів та принципи її побудови	Файлові, завантажувальні (бутові) та файлово-завантажувальні віруси. Макровіруси та мережні віруси. Класифікаційний код вірусу. Дескриптор вірусу. Сигнатура вірусу.
Тема 4. Алгоритми роботи вірусів	Резидентність, використання стелс-алгоритмів, самошифрування й поліморфізм, використання нестандартних прийомів.
Тема 5. Основи низькорівневого програмування	Прості приклади асемблерних програм. Основні типи даних. Контроль за зміною регістрів і прапорів. Основні арифметичні опера- ції. Основні логічні операції. Операції зі стеком. Безумовні та умовні переходи. Цикли. Базова техніка використання переривань.
Тема 6. Антивірусне програмне забезпечення	Поняття про антивірусне програмне забезпечення. Класифікація антивірусного програмного забезпечення.
Тема 7. Принципи роботи антивірусних програм.	Антивірусні програми та особливості їх роботи. Методика використання антивірусних програм.
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, відповідно до графіку навчального процесу. Підсумкова оцінка заліку виставляється як загальна сума балів, набраних за результатами поточного контролю.

Накопичування рейтингових балів з навчальної дисципліни	
Види навчальної роботи	**Мах кількість балів**
Практичні завдання (5 пр.з. по 5 б.)	25
Модульні контрольні роботи (2 по 15 балів)	30
Тестування (2 тестування по 10 б.)	20
Індивідуальне завдання	25
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

Основна:

1. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. Посібник. Дніпро: Дніпроп. держ. унт. внутріш. справ, 2020. 144 с.
2. Інформаційна безпека держави : навч. посіб. В. М. Рудницький та ін. ; Черкас. держ. технол. ун-т. Харків : ДІСА ПЛЮС, 2018. 358 с.
3. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.
4. Інформаційна безпека. Підручник В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.
5. Ситник Г. П., Орел М. Г. Національна безпека в контексті європейської інтеграції України: підручник / Г. П. Ситник, М. Г. Орел; за ред. Г. П. Ситника. – К.: Міжрегіональна Академія управління персоналом, 2021. – 372 с.

Додаткова:

1. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С. Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6 2. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом "Родовід", 2014. – 428 с.
2. Дронюк І. М. Технології захисту інформації на матеріальних носіях Монографія. Львів : Видавництво Львівської політехніки, 2017. 200 с
3. Тарнавський, Ю. А. Технології захисту інформації [Електронний ресурс] : підручник для студентів спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в

інформаційних системах» / Ю. А. Тарнавський ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с

4. Писарчук О.О. Основи захисту інформації : навчальний посібник / О.О. Писарчук, Ю. Г. Даник, С. Г. Вдовенко та ін. – Житомир : ЖВІ ДУТ, 2015. – 226 с

Web-ресурси:

1. Комп’ютерні віруси та як від них захиститися: поради кіберполіції. 2024р. URL: https://cyberpolice.gov.ua/article/kompyuterni-virusy-ta-yak-vid-nyx-zaxystytysya-porady-kiberpolicziyi-6568/

2. Топ-10 комп’ютерних вірусів, які призвели до величезних збитків. URL: https://10guards.com/ua/articles/10-worst-computer-viruses-in-history/.

3. Що таке комп'ютерні віруси? Інструменти для виявлення та запобігання атак. URL: https://gridinsoft.ua/virus.

4. Цікаві факти про комп'ютерні віруси. URL: https://www.miyklas.com.ua/p/informatica/9-klas/programne-zabezpechennia-ta-informatciina-bezpeka-327110/osnovi-zakhistu-danikh-327187/re-a26ed609-33cb-4cb2-92e1-8dfe2409ad85.