

ОСНОВИ КІБЕРБЕЗПЕКИ

СИЛАБУС

Шифр і назва спеціальності	122 Комп'ютерні науки	Інститут / факультет	Факультет комп'ютерних наук і програмної інженерії
Назва програми	«Комп'ютерні науки та інтелектуальні системи» (Innovation Campus)	Кафедра	Кафедра програмної інженерії та інформаційних технологій управління
Тип програми	Освітньо-професійна	Мова навчання	Українська

Викладач

Євсеєв Сергій Петрович

Serhii.Yevseiev@hneu.net



Доктор технічних наук, проф., професор кафедри програмної інженерії та інформаційних технологій управління НТУ «ХПІ». Підготував і опублікував понад 295 наукових та навчально-методичних праць (Google Scholar: https://scholar.google.com/citations?hl=ru&user=Y4kNr38AAAAJ&view_op=list_works&sortby=pubdate; ORCID <https://orcid.org/0000-0003-1647-644>; Scopus: <https://www.scopus.com/authid/detail.uri?authorId=57190440690>; Publons: <https://publons.com/researcher/1527869/serhii-yevseiev/>).
Провідний лектор з курсів: *Основи кібербезпеки (українською мовою)*

Загальна інформація про курс

Анотація	Курс «Основи кібербезпеки» є навчальною дисципліною з циклу спеціальної обов'язкової підготовки за спеціальністю 126 «Інформаційні системи та технології». Вона викладається у шостому семестрі в обсязі 90 годин (3 кредити ECTS), зокрема: лекції – 16 годин, лабораторні заняття – 32 години, самостійна робота – 42 години. Індивідуальних завдань не передбачено. Вивчення дисципліни завершується екзаменом.					
Цілі курсу	Навчання студентів принципам побудови систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення надання основних послуг безпеки інформації в кіберпросторі, проведення аудиту поточного стану інформаційної безпеки.					
Формат	Лекції, лабораторні заняття. Поточний контроль – лабораторні роботи, проміжний модульний контроль. Підсумковий контроль – екзамен.					
Семестр	6					

Обсяг (кредити) / Тип курсу (обов'язковий / вибірковий)	3 / Обов'язковий	Лекції (години)	16	Лабораторні заняття (години)	32	Самостійна робота (години)	42
--	------------------	-----------------	----	------------------------------	----	----------------------------	----

Програмні компетентності	ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК6. Здатність вчитися й оволодівати сучасними знаннями. СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури						
--------------------------	---	--	--	--	--	--	--

Результати навчання	Методи викладання та навчання	Форми оцінювання (поточне оцінювання CAS, підсумкове оцінювання FAS)
ПР15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних	Інтерактивні лекції з презентаціями, дискусії, лабораторні заняття, командна робота, кейс-метод, метод зворотного зв'язку з боку студентів, проблемне навчання	Письмові індивідуальні завдання до лабораторних робіт (CAS), оцінювання знань на лабораторних заняттях (CAS), підсумковий/семестровий контроль у формі семестрового екзамену, відповідно до графіку навчального процесу (FAS)

СИСТЕМА ОЦІНЮВАННЯ

Розподіл балів для оцінювання успішності студента	Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	Нарахування балів	100% підсумкове оцінювання у вигляді екзамену (36%) та поточного оцінювання (64%). 36% екзамен 64% поточне оцінювання: Модуль №1 (12%) Модуль №2 (12%) Лабораторні роботи (40%) Лабораторна робота № 1 (5%) Лабораторна робота № 2 (5%) Лабораторна робота № 3 (5%) Лабораторна робота № 4 (5%) Лабораторна робота № 5 (5%) Лабораторна робота № 6 (5%) Лабораторна робота № 7 (5%) Лабораторна робота № 8 (5%)
	90-100	A	відмінно		
	82-89	B	добре		
	74-81	C			
	64-73	D	задовільно		
	60-63	E			
	35-59	FX	незадовільно з можливістю повторного складання		
	0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни		

Політика курсу	Студент зобов'язаний відвідувати всі заняття згідно навчального розкладу та дотримуватися норм академічної етики. Для вивчення дисципліни необхідно мати власний персональний комп'ютер та/або використовувати комп'ютери обчислювального центру кафедри. Студент повинен працювати з обов'язковою та додатковою літературою, зокрема з інформаційними ресурсами в Інтернеті. Усі лабораторні роботи мають бути виконані та здані студентом протягом семестру, у якому викладається дисципліна, до початку екзаменаційної сесії. Без особистої присутності студента підсумковий контроль не проводиться.
-----------------------	--

Структура та зміст курсу

Тема	Лабораторна робота	Самостійна робота
Тема 1 Поняття кібербезпеки держави та складових національних інтересів України в кібербезпеці	Лабораторна робота 1	Розгортання операційної системи для проведення аудиту інформаційної безпеки комп'ютерних мереж та інформаційних систем
Тема 2 Аналіз ризиків в області кібербезпеки. Класифікація кіберзагроз. Практичні моделі	Лабораторна робота 2	Інструменти прихованого збору технічної інформації з інформаційної системи або комп'ютерної мережі
		Основні етапи проведення внутрішнього аудиту з інформаційної безпеки
		Ознайомлення з основними каналами витоку інформації. Основні принципи формування класифікаторів комп'ютерних інцидентів, кіберзагроз

	розмежування прав доступу				
Тема 3	Механізми забезпечення конфіденційності та цілісності даних	Лабораторна робота 3	Дослідження сучасних блочних симетричних шифрів та режимів шифрування. Дослідження сучасних асиметричних криптосистем шифрування		Основні механізми забезпечення цілісності в інформаційних системах
Тема 4	Механізми забезпечення автентифікації	Лабораторна робота 4	Дослідження електронного цифрового підпису. ЦП Ель Гамалія, ДСТУ 4145, ECDSA. Дослідження вразливостей системи або мережі за допомогою спеціалізованого сканера вразливостей – Nessus		Основні спеціальні геш-функції. Стандарти цифрового підпису, їх класифікація
Тема 5	Основні напрямки розвитку сучасної криптографії	Лабораторна робота 5	Стеганографічні методи захисту інформації		Методи стеганографії у просторовій та частотній області
Тема 6	Механізми та протоколи керування ключами в ІВК	Лабораторна робота 6	Статистичні дослідження генераторів випадкових та псевдовипадкових послідовностей за методикою NIST		Основні протоколи PKI на основі симетричної та несиметричної криптографії
Тема 7	Технології аналізу ризиків	Лабораторна робота 7	Визначення вразливостей веб ресурсів та веб додатків. Сканер вразливостей – Vega		
Тема 8	Аналіз ризиків в управлінні неформативною безпекою	Лабораторна робота 8	Збір технічної та чуттєвої інформації за допомогою ПЗ класу – сніфери. Засіб дослідження вразливостей безпроводних мереж Wi-Fi – Aircrack-ng		Методики аналізу ризиків

Література

- Євсєєв С.П., Остапов С.Е., Король О.Г. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678.
2. Р. В. Грищук, та Ю. Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016..
3. Ленков С.В. Методы и средства защиты информации. В 2-х томах/ С. В. Ленков, Д. А. Перегудов, В. А. Хорошко.– К.: Арий, 2008. – Т.ІІ. Информационная безопасность. – 344 с.

4. Баранов А.А., Интернет речей: теоретико-методологічні основи правового регулювання. Том І. Сфери застосування, ризики і бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с.
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. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. – Харків, Видавництво: Форт, 2012. – 878.
7. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник: В 2 т. / В. В. Поповский, А. В. Персиков. – Харьков: ООО “Компания СМІТ”, 2006. – Т.1. – 292 с.
8. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник: В 2 т. / В. В. Поповский, А. В. Персиков. – Харьков: ООО “Компания СМІТ”, 2006. – Т.2. – 252 с.
9. Стратегія кібербезпеки України” (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016).
- Євсєєв С.П. Лабораторний практикум з дисципліни “Технології захисту інформації” [Електронний ресурс]. – Режим доступу: ntumoodle.com

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

10. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Електронний ресурс]. Доступно: <http://lindex.net.ua/ua/shop/bibl/500/doc/11423>.
11. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Електронний ресурс]. Доступно: <http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekioiu-informatsiinih-tiekhnologhii>.
12. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Електронний ресурс]. Доступно: <http://lindex.net.ua/ua/shop/bibl/500/doc/11425>
13. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту. [Електронний ресурс]. Доступно: <http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005>
14. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Електронний ресурс]. доступно: <http://lindex.net.ua/ua/shop/bibl/500/doc/11427>
15. <http://dstsi.gov.ua>.

Норми академічної етики

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність

Силабус за змістом повністю відповідає робочій програмі курсу.