НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Навчально-науковий інститут кібернетики, інформаційних технологій та інженерії

04-04-37S

СИЛАБУС **SYLLABUS**	**Безпека інформаційних систем та захист інформації**	
	Information systems security and information protection	
Шифр за ОП Code in Degree Programme	**ОК 17**	
Освітній рівень Level of Education	**Бакалаврський (перший)**	
	Bachelor's (first)	
Галузь знань Field of Knowledge	**12**	**Інформаційні технології** **Information Technology**
Спеціальність Field of Study	**122**	**Комп'ютерні науки** **Computer science**
Освітня програма Degree Programme	**Комп'ютерні науки**	
	Computer science	

РІВНЕ – 2024

Силабус навчальної дисципліни «Безпека інформаційних систем та захист інформації» для здобувачів вищої освіти ступеня «бакалавр», які навчаються за освітньо-професійною програмою «Комп'ютерні науки» спеціальності 122 «Комп'ютерні науки». Рівне. НУВГП. 2024. 14 стор.

ОП на сайті університету: *https://ep3.nuwm.edu.ua/23461/*.

Розробники силабусу: *Назарук Віталій Дмитрович, кандидат технічних наук, старший викладач кафедри обчислювальної техніки*

Силабус схвалений на засіданні кафедри обчислювальної техніки
Протокол №1 від 27 серпня 2024 року

Завідувач кафедри: *Сидор Андрій Іванович, кандидат технічних наук, доцент*

Керівник (гарант) освітньої програми: *Каштан Сергій Степанович*, *кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук та прикладної математики*

Схвалено науково-методичною радою з якості ННІ кібернетики, інформаційних технологій та інженерії
Протокол №9 від 30 серпня 2024 року

Голова науково-методичної ради з якості ННІ: *Мартинюк Петро Миколайович*, *доктор технічних наук, професор, директор* ННІ кібернетики, інформаційних технологій та інженерії

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Безпека інформаційних систем та захист інформації»

ЗАГАЛЬНА ІНФОРМАЦІЯ	
Ступінь вищої освіти	*бакалавр*
Освітня програма	*Комп'ютерні науки*
Спеціальність	*122 Комп'ютерні науки*
Рік навчання, семестр	*4-й рік навчання, 7-й семестр*
Кількість кредитів	*4*
Лекції:	*24 год.*
Лабораторні заняття:	*24 год.*
Самостійна робота:	*72 год.*
Курсова робота:	-
Форма навчання	*денна, заочна*
Форма підсумкового контролю	*екзамен*
Мова викладання	*державна*

ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА	
Лектор 	**Назарук Віталій Дмитрович**, канд. техн. наук, старший викладач кафедри обчислювальної техніки v.d.nazaruk@nuwm.edu.ua
Вікіситет	*http://wiki.nuwm.edu.ua/index.php/%D0%9D%D0%B0%D0%B7%D0%B0%D1%80%D1%83%D0%BA_%D0%92%D1%96%D1%82%D0%B0%D0%BB%D1%96%D0%B9_%D0%94%D0%BC%D0%B8%D1%82%D1%80%D0%BE%D0%B2%D0%B8%D1%87*
Як комунікувати	https://exam.nuwm.edu.ua/course/view.php?id=3019 Кафедра обчислювальної техніки: каб. 128, **e-mail:** kaf-ot@nuwm.edu.ua https://nuwm.edu.ua/nni-akot/kaf-ot Електроний журнал: http://desk.nuwm.edu.ua/ Розклад занять: http://desk.nuwm.edu.ua/cgi-bin/timetable.cgi Консультації (дистанційно) на платформі Google (Hangouts) Meet: https://meet.google.com/ajg-cokm-mcv?authuser=0
ІНФОРМАЦІЯ ПРО ОСВІТНЮ КОМПОНЕНТУ	

Мета та завдання

Навчальна дисципліна «Безпека інформаційних систем та захист інформації» входить до циклу загальної підготовки студентів-бакалаврів і є однією з ключових складових фундаментальної підготовки фахівців в галузі інформаційних технологій.
Навчальний курс призначений для вивчення основних засобів та заходів захисту інформації в інформаційних системах, в якому класифіковано загрози для інформації за критеріями цілісності, конфіденційності та доступності, методів та засобів їх локалізації та блокування. Подано основні принципи формування систем технічного та криптографічного захисту інформації. Надано описи та розглянуто принципи дії сучасних криптоалгоритмів, засобів хешування, генерації та технологій електронного цифрового підпису.

Мета дисципліни полягає в отриманні здобувачами вищої освіти теоретичних знань та практичних навичок побудови захищених інформаційних систем на основі сучасних засобів технічного та криптографічного захисту інформації.
Основними завданнями є формування системного підходу до побудови захищених інформаційних систем, набуття навиків блокування технічних каналів витоку інформації,
отримання знань порядку застосування методів захисту від несанкціонованого доступу

Передумови вивчення

Передумовами вивчення навчальної дисципліни Безпека інформаційних систем та захист інформації є освоєння здобувачами вищої освіти наступних навчальних дисциплін: комп'ютерні мережі, методика навчання інформатики, веб-технології та веб-дизайн, операційні системи та системне програмне забезпечення.

Посилання на розміщення освітнього компоненту на навчальній платформі Moodle

https://exam.nuwm.edu.ua/course/view.php?id=2792

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.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК6. Здатність вчитися й оволодівати сучасними знаннями.
ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК16. Здатність до самостійності, ініціативності, адаптації та дій в нових ситуаціях (креативність).
ФК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

Програмні результати навчання (ПРН). Результати навчання (РН)

ПРН15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

Структура та зміст освітнього компонента

теми, деталізовані ПРН, завдання, форми проведення занять, види навчальної роботи студента, методи та технології навчання, засоби навчання, перелік навчальних матеріалів, які повинен опанувати/ознайомитись студент перед заняттям та інше

Перелік соціальних, «м'яких» навичок (soft skills)

– Уміння планувати робочий час для виконання самостійної роботи, опрацювання літератури та пошуку необхідної інформації.
– Здатність комунікувати, зрозуміло та аргументовано доносити свою точку зору.
– Бажання постійно навчатись, освоювати нові технології, виробляти потребу в отриманні нових знань.
– Вміння працювати в команді на спільний результат.
– Здатність до критичного мислення при обговоренні матеріалів навчання, перевірки результатів лабораторних робіт.

Форми та методи навчання

Форми навчання: очна та дистанційна.
Методи навчання: інтерактивні, активні, наочні, практичні.

Інструменти, обладнання, програмне забезпечення

Комп'ютерна лабораторія ASUS U500MAAMD Ryzen 3-5300G + Lenovo Think Vision E22-20 (62A4MAT4UA) – 15 комплектів
Програмне забезпечення: Windows 10, Office 2019, КЗЗ «Лоза», версія 4.1.1;
Обладнання: Селективний мікровольтметр STV 301-2, Феромагнітна антена FSA 101, генератор радіочастотного шуму мобільний "РІАС-1ГМ" / 8 Вт.

Тема 1. Поняття інформації. Загрози для інформації. Основні види технічних засобів розвідки.

Кільк. годин:
2 год лекцій;
9 год. сам. роб.

Література:
1, с.56-65; 2, с.21-25;
3, с. 69-75; 4, с.125-141;
5, с.123-147

Лінк на Moodle:
https://exam.nuwm.edu.ua/course/view.php?id=2792

Опис теми: **Лекція 1.** Поняття інформації. Загрози для інформації. Основні види технічних засобів розвідки.
Визначення інформації. Ідентифікація загроз для інформації. Класифікація основних форм розвідувальної діяльності. Види технічних засобів розвідки. Основні принципи добування інформації за допомогою технічних засобів
Сам. роб. Вивчення основних вимог щодо захисту від несанкціонованого доступу до інформації.

Тема 2. Технічні каналів витоку інформації. Класифікація. Види. Модель технічного каналу витоку інформації.

Кільк. годин:
2 год лекцій;
2 год. лаб. роб.;
9 год. сам. роб.

Література:
1, с. 131-147;

Лінк на Moodle:
https://exam.nuwm.edu.ua/course/view.php?id=2792

Опис теми: **Лекція 2.** Технічні каналів витоку інформації. Класифікація. Види. Модель технічного каналу витоку інформації.
Поняття технічного каналу витоку інформації. Класифікація ТКВІ. Небезпечні сигнали. Контрольована зона.
Лаб. роб. 1. Визначення амплітуди гармонік та побудова спектра побічних електромагнітних випромінювань монітора комп'ютера..
Сам. роб. Вивчення засобів та методів виявлення небезпечних сигналів на об'єктах інформаційної діяльності

Тема 3. Технічні канали витоку інформації. Побічні електромагнітні випромінювання.

Кільк. годин:
2 год лекцій;
2 год. лаб. роб.;
9 год. сам. роб.

Література:
1, с.78-98; 2, с.113-138.

Лінк на Moodle:
https://exam.nuwm.edu.ua/course/view.php?id=2792

Опис теми: **Лекція 3.** Технічні канали витоку інформації. Побічні електромагнітні випромінювання.
Фізичні основи побічних електромагнітних випромінювань. Рівняння Максвелла. Електрична та магнітна складові електромагнітного поля. Спектральна щільність випромінювання.
Лаб. роб. 2. Створення широкосмугового сигналу завади для захисту від витоку за рахунок побічних електромагнітних випромінювань.
Сам. роб. Вивчення природи утворення та розповсюдження електромагнітних випромінювань.

Тема 4. Технічні засоби захисту інформації. Захист інформації від технічних каналів витоку. Вимоги нормативних документів з питань технічного захисту інформації.

Кільк. годин:
2 год лекцій;
2 год. лаб. роб.;
9 год. сам. роб.

Література:
1, с.115-173; 2, с.62-86; 3, с.19-34; 4, с.32-76;

Лінк на Moodle:
https://exam.nuwm.edu.ua/course/view.php?id=2792

Опис теми: **Лекція 4.** Технічні засоби захисту інформації. Захист інформації від технічних каналів витоку. Вимоги нормативних документів з питань технічного захисту інформації.
Локалізація побічних електромагнітних випромінювань. Захист від параметричних каналів витоку інформації.
Лаб. роб. 3. . Дослідження політики облікових записів ОС WINDOWS
Сам. роб. Розробка плану захисту інформації на об'єкті інформаційної діяльності

Тема 5. Програмні засоби захисту інформації. Підсистеми захисту в операційних системах.

Кільк. годин:
2 год лекцій;
2 год. лаб. роб.;
9 год. сам. роб.

Література:
1, с.19-45; 3, с.138-153; 4, с.62-96.

Лінк на Moodle:
https://exam.nuwm.edu.ua/course/view.php?id=2792

Опис теми: **Лекція 5.** Програмні засоби захисту інформації. Підсистеми захисту в операційних системах. *Локальна підсистема безпеки. Журнал подій. Облікові записи. Диспетчер завдань. Ідентифікатор безпеки SID*
Лаб. роб. 4 Вивчення основних функцій комплексу засобів захисту «Гриф-3».
Сам. роб. Вивчення політик безпеки операційної системи LINUX.

Тема 6. Комплекси засобів захисту для автоматизованих систем.

Кільк. годин:
2 год лекцій;
8 год. лаб. роб.;
9 год. сам. роб.

Література:
1, с.48-87; 3, с.408-463; 4, с.214-242; 5, с.179-207

Лінк на Moodle:
https://exam.nuwm.edu.ua/course/view.php?id=2792

Опис теми: **Лекція 6.** Комплекси засобів захисту для автоматизованих систем.
Функції комплексів засобів захисту. Функціональний профіль захищеності і рівень гарантій. Політики функціональних послуг безпеки. Монітор безпеки.
Лаб. роб. 5. Вивчення функціональних характеристик комплексу засобів захисту «Лоза-1».
Лаб. роб. 6. Інсталяція та деінсталяція комплексу засобів
захисту «Лоза-1»
Лаб. роб. 7. Робота з функціоналом комплексу засобів захисту «Лоза-1»
Лаб. роб. 8. Робота з переліком користувачів комплексу засобів захисту «Лоза-1»
Сам. роб. Функціонал адміністратора КЗЗ та адміністратора безпеки комплексу
засобів захисту від несанкціонованого доступу.

Тема 7. Криптографічний захист інформації. Основні вимоги до криптографічних систем. Поняття криптоалгоритму. Симетричні криптоалгоритми

Кільк. годин:
2 год лекцій;
2 год. лаб. роб.;
9 год. сам. роб.

Література:
1, с.188-204;
2, с.239-337;
3, с.243-307;
4, с.240-264

Лінк на Moodle:
https://exam.nuwm.edu.ua/course/view.php?id=2792

Опис теми: **Лекція 7.** Криптографічний захист інформації. Основні вимоги до криптографічних систем. Поняття криптоалгоритму
Історія криптології. Основні вимоги до криптосистем. Загальна схема симетричного шифрування. Методи заміни. Пропорційні шифри. Багатоалфавітна підстановки.
Лаб. роб. 9. Основи криптографічного захисту інформації. Симетричні криптоалгоритми**.**
Сам. роб. Симетричні криптоалгоритми докомп'ютерного періоду

Тема 8. Мережа Фейстеля. Криптоалгоритм DES

Кільк. годин:
2 год лекцій;
9 год. сам. роб

Література:
1, с.205-234;
2, с.337-356;
3, с.308-317;
4, с.265-286

Лінк на Moodle:
https://exam.nuwm.edu.ua/course/view.php?id=2792

Опис теми: **Лекція 8.** Мережа Фейстеля. Криптоалгоритм DES
Вимоги до блокового криптоалгоритму. Алгоритм мережі Фейстеля. Криптоалгоритм DES – загальна схема, структура раунду.
Сам. роб. Симетричні криптоалгоритми на основі мережі Фейстеля.

Тема 9. Криптоалгоритм ГОСТ 28147-89. Типові схеми. Структура раунду ГОСТ 28147-89. Алгоритми шифрування та розшифрування

Кільк. годин:	Література:	Лінк на Moodle:
2 год лекцій; 4 год. сам. роб	1, с.235-254; 2, с.357-374.	https://exam.nuwm.edu.ua/course/view.php?id=2792

Опис теми: **Лекція 9.** Криптоалгоритм ГОСТ 28147-89. Типові схеми. Структура раунду ГОСТ 28147-89. Алгоритми шифрування та розшифрування
Загальні відомості. Структура раунду. Процедури шифрування та розшифрування. Основні режими шифрування. Технології гамування та імітовставки.
Сам. роб. Застосування криптоалгоритму ГОСТ 28147-89 в для криптосистем різного рівня стійкості.

Тема 10. Асиметричні криптоалгоритми. Алгоритм Діффі-Хеллмана. Криптоалгоритм RSA. Основні відомості. Шифрування та розшифрування. Практичне використання

Кільк. годин:	Література:	Лінк на Moodle:
2 год лекцій; 4 год. сам. роб	1, с.284-325; 2, с.395-426;	https://exam.nuwm.edu.ua/course/view.php?id=2792

Опис теми: **Лекція 10** Асиметричні криптоалгоритми. Алгоритм Діффі-Хеллмана. Криптоалгоритм RSA. Основні відомості. Шифрування та розшифрування. Практичне використання
Алгоритм Діффі-Хелмана - основні відомості, приклади обчислень, практичне використання. Криптоалгоритм RSA - основні відомості, приклади обчислень, практичне використання.
Лаб. роб. 10 Генерація спільного закритого ключа для симетричного шифрування за алгоритмом Діффі-Хелмана
Лаб. роб. 11 Розрахунок параметрів відкритого та закритого ключа асиметричного криптоалгоритму RSA. Шифрування та розшифрування повідомлення за допомогою розрахованих параметрів.
Лаб. роб. 12 Шифрування інформації за допомогою асиметричних криптоалгоритмів в програмному середовищі Gpg4win
Сам. роб. Асиметричні криптоалгоритми на еліптичних кривих

Порядок та критерії оцінювання	
За поточну (практичну) складову оцінювання 24 бали	За модульний (теоретичний) контроль знань (МК2) 20 балів
Усього за поточну (практичну) складову оцінювання, балів	60

Усього за модульний контроль, або екзамен, балів	40
Усього за дисципліну, балів	100
За поточну (практичну) складову оцінювання 24 бали	За модульний (теоретичний) контроль знань (МК2) 20 балів
Методи оцінювання та структура оцінки *COURSE GRADE COMPOSITION*	Для оцінювання рівня знань застосовується 100-бальна шкала оцінювання. Величина рівня засвоєння матеріалу навчання відбувається за такими методами: • поточне опитування після вивчення кожної теми; • оцінка за підготовку, виконання та захист лабораторної роботи; • оцінка за самостійну роботу; • підсумковий контроль у вигляді тестування: 2 модулі або екзамен. Основними показниками, що характеризують рівень знань студента за результатами вивчення дисципліни є: • виконання всіх видів навчальної роботи, що передбачені цим силабусом; • рівень знань навчального матеріалу за змістом навчальної дисципліни; • вміння студента презентувати свої знання, навички та отриманий практичний досвід; • вміння проводити аналіз результатів виконання лабораторних робіт та захищати одержані результати. Оцінювання результатів роботи проводиться у % від кількості балів, виділених на завдання, із заокругленням до цілого числа: 0% – завдання не виконано; 40% – завдання виконано частково та містить суттєві помилки методичного або розрахункового характеру; 60% – завдання виконано повністю, але містить суттєві помилки у розрахунках або в методиці; 80% – завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки; 100% – завдання виконано правильно, вчасно і без зауважень. ***Поточна (практична)*** складова оцінки (не більше, ніж 60 балів) нараховується за виконання лабораторних робіт до 5 балів за кожну лабораторну роботу; виконання самостійної роботи (реферат, презентація – до 5 балів; виконання лабораторних робіт з програмною реалізацією – до 5 балів). ***Підсумкова (теоретична)*** складова оцінки курсу (не більше, ніж 40 балів) нараховується

за модульний контроль (МК1 – до 20 балів; МК2 – до 20 балів) або за екзамен (ЕКЗ – до 40 балів). Модульні контролі та екзамен проводяться через ННЦНО НУВГП у формі комп'ютерного тестування на платформі Moodle. МК1, МК2 і ЕКЗ містять по 27 тестових завдань: 24 завдання першого рівня складності, 2 завдань другого рівня складності і 1 завдання третього рівня складності. За одне завдання першого рівня складності студент може отримати до 0,5 бала (МК1 і МК2) або 1 бал (ЕКЗ); за одне завдання другого рівня складності студент може отримати до 02 балів (МК1 і МК2) або до 4 балів (ЕКЗ); за одне завдання третього рівня складності – до 4 балів (МК1 і МК2) або до 8 балів (ЕКЗ).

Додаткові бали (не більше, ніж 20):

– за підготовку тез на наукову конференцію за тематикою навчальної дисципліни – до 10 балів;

– за подання статті в збірник наукових праць – до 20 балів.

Загальна інтегральна оцінка курсу розраховується як арифметична сума набраних балів (не більше, ніж 100) за всі види навчальних та додаткових завдань.

Шкала загальної оцінки курсу

Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою
90-100	відмінно
82-89	добре
74-81	добре
64-73	задовільно
60-63	задовільно
0-59	незадовільно

Інформаційні ресурси

Рекомендована література

Основна

1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средст-ва защиты информации . Том 1. Несанкционированное получение информации Киев: Арий 2008, 326с.
2. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средст-ва защиты информации . Том 2. Информционная безопасность Ки-ев: Арий 2008 385с.
3. Поповский В.В., Персиков А.В. Основы криптографической защиты информации в телекоммуникационных системах Харьков: СМИТ 2010 465с.
4. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем К, «BHV», 2009. - 608с.

Допоміжна

1. Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369 (Перевод В.Ф.Писаренко)
2. Фергюсон Н., Шнайер Б. Практическая криптография. : Пер. с англ. — М.: Издательский дом "Вильямс", 2005. — 424 с. : ил.
3. Хорошков В. А., Чекатков А. А. Методы и средства защиты ин-формации / Под ред. Ю. С. Ковтанюка – К.: Издательство Юниор, 2003.- 504с., ил.
4. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. - М.: "Триумф", 2002.

Інформаційні ресурси в Інтернет

1. Національна бібліотека ім. В. І. Вернадського. URL: http://www.nbuv.gov.ua/e-resources/, http://www.nbuv.gov.ua/webnavigator/
2. Рівненська обласна універсальна наукова бібліотека (м. Рівне, майдан Короленка, 6). URL: http://www.libr.rv.ua/
3. Рівненська централізована бібліотечна система (м. Рівне, вул. Київська, 44). URL: http://cbs.rv.ua/
4. Наукова бібліотека НУВГП (м. Рівне, вул. Олекси Новака, 75). URL: http://nuwm.edu.ua/naukova-biblioteka/, http://nuwm.edu.ua/MySql/page_lib.php
5. Цифровий репозиторій НУВГП. URL: http://ep3.nuwm.edu.ua.

Дедлайни та перескладання

Завдання до лабораторних та самостійних робіт з відповідної теми повинні бути виконані і здані на оцінювання протягом 10 днів з дати заняття. При порушення термінів кількість балів знижується на 10%. Кінцевим терміном здачі завдань є останній робочий день навчального семестру.
Порядок повторного проходження контрольних заходів у НУВГП врегульовано «Положенням про семестровий поточний та підсумковий контроль навчальних досягнень здобувачів вищої освіти»: http://ep3.nuwm.edu.ua/5040/.
Усі перездачі проходять за погодженням з директором ННІ. Правила ННЦНО стосовно повторного тестування наведено у документах: http://nuwm.edu.ua/strukturni-pidrozdili/navch-nauk-tsentr-nezalezhnoho-otsiniuvannia-znan/dokumenti.
Перша перездача проводиться через ННЦНО згідно з розкладом перездач, який розміщено в додатку Мій НУВГП та ПС-Студент WEB: http://desk.nuwm.edu.ua/cgi-bin/shell.cgi?n=999.
У випадку отримання незадовільної оцінки, здобувач направляється на комісію з перездачі дисципліни, яка формується деканатом ННІ. Після трьох невдалих спроб здачі семестрового підсумкового контролю з навчальної дисципліни вважається, що здобувач має академічну заборгованість. Рішення про повторне вивчення навчальної дисципліни або відрахування здобувача приймає ректор на підставі звернення директора ННІ, як це передбачено «Порядком ліквідації академічних заборгованостей у НУВГП»: http://ep3.nuwm.edu.ua/id/eprint/4273.
У випадку нездачі підсумкового контролю через хворобу чи з інших поважних причин, здобувач має написати заяву на ім'я директора ННІ для зміни строків сесії.

Неформальна та інформальна освіта

Визнання (перезарахування) результатів навчання, здобутих у неформальній та інформальній освіті, відбувається відповідно до «Положення про неформальну та інформальну освіту в НУВГП»: http://nuwm.edu.ua/sp/neformalna-osvita
Здобувачі можуть пройти відкриті онлайн курси, близькі за темою до даної навчальної дисципліни, таких платформ як Coursera, Prometheus, edEx, edEra, VUMOnline, FutureLearn тощо.
Зокрема, рекомендується курс на платформі Coursera: **Cybersecurity Compliance Framework & System Administration** https://www.coursera.org/learn/cybersecurity-compliance-framework-system-administration

Правила академічної доброчесності

Викладач та здобувачі несуть спільну відповідальність за створення сприятливого творчого навчального середовища, яке базується на взаємній повазі.
До кожного заняття здобувачі повинні наперед ознайомитися з матеріалами та інформаційними ресурсами, наведеними у методичних вказівках і розміщеними на сторінці дисципліни в Moodle.
Здобувачі освіти повинні дотримуватися Кодексу честі студентів. http://nuwm.edu.ua/strukturni-pidrozdili/vvrsdev/dokumenti
Принцип студентоцентризму передбачає розуміння серйозності ставлення до академічної недоброчесності та неправомірної поведінки. Студенти мають самостійно виконувати і здавати на оцінювання лише результати власних зусиль та оригінальної праці.
При виконанні практичних робіт з дисципліни студентам рекомендується працювати в навчальних групах, порівнювати отримані результати та обговорювати застосовувані методи. Однак виконуючи поставлені завдання, студенти повинні індивідуально здійснити кожен розрахунок. Обмін виконаними завданнями чи їх частинами у формі тексту, таблиці, програмного коду чи у будь-якій іншій формі є недопустимим. Не існує прийнятного приводу для плагіату чи обману. Здобувачі освіти не можуть копіювати виконані завдання у інших студентів, ділитися виконаними завданнями з іншими студентами і мають дотримуватися Положення про виявлення та запобігання академічного плагіату в НУВГП http://nuwm.edu.ua/sp/akademichna-dobrochesnistj
У випадку плагіату при виконанні завдання здобувач не отримує бали і повинен виконати завдання повторно.
Перевірка дотримання доброчесності під час модульного та підсумкового контролю може здійснюватися засобами відеонагляду.
Здобувачі можуть робити аудіозапис аудиторного заняття для свого особистого освітнього використання тільки за погодженням з викладачем і не мають права розміщувати такий запис в соціальних мережах.

Вимоги до відвідування

Здобувачі вищої освіти зобов'язані відвідувати усі лекційні та практичні заняття з дисципліни згідно розкладу http://desk.nuwm.edu.ua/cgi-bin/timetable.cgi
Відвідування консультацій не обов'язкове.
У випадку відсутності з поважних причин (індивідуальний план, лікарняний, мобільність тощо) здобувач самостійно опрацьовує теоретичний матеріал і виконує завдання з відповідної практичної роботи.
Завдання до практичних робіт розміщено на платформі Moodle https://exam.nuwm.edu.ua/course/view.php?id=1818
Файл (файли) із виконаними розрахунками здобувач прикріплює до відповідних завдань на платформі Moodle. Захист роботи відбувається на наступному занятті, консультації або онлайн у відеорежимі.
На лекціях і практичних заняттях студенти можуть використовувати свої ноутбуки, планшети чи смартфони для роботи.

Оновлення

Силабус переглядається кожного навчального року з урахуванням рекомендацій здобувачів освіти, які вони можуть подати під час онлайн опитування, з метою оновлення (осучаснення) змісту навчальної дисципліни на основі наукових досягнень і сучасних практик у галузі інформаційних технологій.

Академічна мобільність. Інтернаціоналізація

Програма національних обмінів «Плацкарт» відповідно до Положення http://ep3.nuwm.edu.ua/13963/ .
За угодами про міжнародну академічну мобільність (Еразмус+ К1), на основі двосторонніх договорів між НУВГП та зарубіжними навчальними закладами

Автор
Старший викладач ОТ Віталій НАЗАРУК

Затверджено

Проректор з науково-педагогічної та навчальної роботи Валерій СОРОКА

документ підписаний КЕП
Номер документа СИЛ №815
Підписувач Сорока Валерій Степанович
Підписувач (дані КЕП):
Сертифікат 3FAA9288358EC003040000009B6C3700C8C2C100