НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Навчально-науковий інститут кібернетики, інформаційних технологій та інженерії

04-04-47S

СИЛАБУС *навчальної дисципліни*		**SYLLABUS**
Безпека та захист комп`ютерних систем		Security and protection of computer systems
Шифр за ОП	ОК-6	Code in Degree Programme
Освітній рівень: бакалаврський (перший)		Level of Education: Master's (second)
Галузь знань Інформаційні технології	12	Field of Knowledge Information Technologies
Спеціальність Комп’ютерна інженерія	123	Field of Study Computer Engineering
Освітня програма: Комп’ютерна інженерія		Degree Programme: Computer Engineering

РІВНЕ – 2024

Силабус навчальної дисципліни «Безпека та захист комп’ютерних систем» для здобувачів вищої освіти ступеня «магістр», які навчаються за освітньо-професійною програмою «Комп’ютерна інженерія», спеціальності «Комп’ютерна інженерія», Рівне. НУВГП. 2024. 12 стор.

ОП на сайті університету: Освітньо-професійна програма "Комп'ютерна інженерія" другого рівня вищої освіти за спеціальністю 123 "Комп'ютерна інженерія" галузі знань 12

Розробник силабусу: Бабич С.В., к.т.н., старший викладач кафедри обчислювальної техніки

Силабус схвалений на засіданні кафедри
Протокол № 1 від “27” серпня 2024 року

В.о. завідувача кафедри: Сидор А.І., к. т. н..

Керівник (гарант) ОП: Круліковський Б.Б., к. т. н., доцент кафедри обчислювальної техніки.

Схвалено науково-методичною радою з якості ННІ
Протокол № 9 від “ 30 ” серпня 2024 року

Голова науково-методичної ради з якості ННІ: Мартинюк П.М., д.т.н., професор

Попередня версія силабусу: відсутня.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ‹ Безпека та захист комп’ютерних систем ›	
ЗАГАЛЬНА ІНФОРМАЦІЯ	
Ступінь вищої освіти	*Магістр*
Освітня програма	Комп’ютерна інженерія
Спеціальність	Комп’ютерна інженерія
Рік навчання, семестр	*1* *2*
Кількість кредитів	*5,5*
Лекції:	*28/6 годин*
Лабораторні заняття:	*28/12 годин*

Самостійна робота:	*109/147 годин*
Курсова робота:	*ні*
Форма навчання	*денна, заочна*
Форма підсумкового контролю	*екзамен*
Мова викладання	*українська*

ІНФОРМАЦІЯ ПРО РОЗРОБНИКА

Лектор	*Бабич Сергій Васильович, к.т.н., ст. викладач кафедри обчислювальної техніки*
ORCID:	*http://orcid.org/ 0000-0002-8669-7288*
Як комунікувати	*s.v.babych@nuwm.edu.ua* *тел. 093-772-13-61*

ІНФОРМАЦІЯ ПРО НАВЧАЛЬНУ ДИСЦИПЛІНУ

Мета та завдання

Дисципліна призначена для набуття студентами здатності забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах і мережах з метою реалізації встановленої політики інформаційної безпеки. Це досягається вивченням теоретичних основ побудови і практики застосування методів та засобів захисту інформації в комп'ютерних системах з метою запобігання несанкціонованому доступи, витоку, руйнації, знищення і модифікації інформації різної категорії шляхом реалізації політики і створення комплексних корпоративних систем захисту інформації.

Метою викладання дисципліни: " Безпека та захист комп'ютерних систем" є: набуття студентами здатності забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах і мережах з метою реалізації встановленої політики інформаційної безпеки.

Мета курсу досягається реалізацією часткових завдань:

- *Вивчення основних положень законодавчої база в сфері захисту інформації в комп'ютерних системах: національні законодавчі акти і стандарти у сфері захисту інформації: категорії, основні положення, порядок і сфера застосування;*

законодавчі акти та стандарти інших держав у сфері захисту інформації;.

- *Визначення складу, організаційних, технічних та програмно-апаратних засобів комплексної системи захисту корпоративної інформації: інформація як об'єкт захисту; категорії інформації, як об'єкту захисту; канали витоку корпоративної інформації; загрози інформації в комп'ютерних системах; модель порушника; методи, методології, засоби, заходи і технології комплексного захисту корпоративної інформації (організаційні заходи, технічний захист інформації, протидія технічним засобам моніторингу).*
- *Класифікація вірусів; алгоритми функціонування вірусів; технології та засоби створення і розповсюдження комп'ютерних вірусів; конструктори вірусів; антивірусне програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів.*
- *Огляд кібернетичних загроз комп'ютерним системам та протидія їм: кібернетична та (і) комп'ютерна атака, поняття, класифікація, модель, зміст етапів; методи і технології організації та реалізації кібернетичних атак; методології, методи і технології протидії кібернетичним атакам; и, метод програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів.*
- *Отримання навичок в сфері криптографічного захисту інформації в комп'ютерних системах: загальні відомості про класичну криптологію, криптографію та криптографічний аналіз; традиційні історичні шифри; алгоритми блочного шифрування; принципи побудови сучасних симетричних криптографічних шифрів та систем; асиметричні криптографічні системи шифрування (сутність та математичні основи; алгоритми та криптографічні системи; технології реалізації та уразливість).*
- *Огляд методів, методологій, технологій і засобів аутентифікації та ідентифікації, як елементів захисту інформації в комп'ютерних системах: методи і технології ідентифікації користувачів; електронний цифровий підпис, центри сертифікації електронних ключів.*

Посилання на розміщення навчальної дисципліни на навчальній платформі Moodle
Курс: Безпека та захист комп'ютерних систем | (nuwm.edu.ua)
Передумови вивчення (місце навчальної дисципліни в структурно-логічній схемі)
Для вивчення даної ОК студентам необхідно мати знання з таких дисциплін: Теорія і технології проєктування спеціалізованих операційних систем, а також вибіркових компонент Вб2.1. або ВБ2.2 *–На матеріалі даної дисципліни ґрунтується вивчення: ОК-11 «Кваліфікаційна магістерська робота».*[a]
Компетентності

СК03. Здатній проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.

СК08. Здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу.

СК11. Здатність обирати ефективні методи розв'язування складних задач комп'ютерної інженерії, критично оцінювати отримані результати та аргументувати прийняті рішення.

СК12. Здатність використовувати та захищати апаратно-програмне забезпечення комп'ютерних, кіберфізичних та спеціалізованих систем.

Результати навчання

РН05. Розробляти і реалізовувати проекти у сфері комп'ютерної інженерії та дотичні до неї міждисциплінарні проекти з урахуванням інженерних, соціальних, економічних, правових та інших аспектів.

РН06. Аналізувати проблематику, ідентифікувати та формулювати конкретні проблеми, що потребують вирішення обирати ефективні методи та їх вирішення.

РН11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп'ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

РН14. Здатність застосувати теоретичні та практичні знання для розв'язання прикладних задач забезпечення захищеності інформаційних технологій, зокрема інтелектуальних та обчислювальних систем.

Структура та зміст навчальної дисципліни

Тема 1. Основні відомості про захист інформації в комп'ютерних системах.

Результати навчання – РН06, РН14.

Опис теми. Основні положення законодавчої база в сфері захисту інформації в комп'ютерних системах: зміст та задачі дисципліни; національні законодавчі акти і стандарти у сфері захисту інформації: категорії, основні положення, порядок і сфера застосування; законодавчі акти та стандарти інших держав у сфері захисту інформації.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 1. Огляд нормативно-правової сфери питання та державних регламентуючих документів.

Тема 2. Організаційні, технічні та програмно-апаратні засоби комплексної системи захисту корпоративної інформації.

Результати навчання – РН06, РН11.

Опис теми. Комплексна система захисту корпоративної інформації. Об'єкт захисту та загрози: інформація як об'єкт захисту; категорії інформації, як об'єкту захисту; канали витоку корпоративної інформації; загрози інформації в комп'ютерних системах;. Комплексна система захисту корпоративної інформації. Склад та структура: модель порушника; методи, методології,

засоби, заходи і технології комплексного захисту корпоративної інформації (організаційні заходи, технічний захист інформації, протидія технічним засобам моніторингу).

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 2. Дослідження процесів створення комплексної системи захисту корпоративної інформації (КСЗІ): Розробка проекту КСЗІ для конкретного об'єкту інформаційної діяльності – комп'ютерної системи (встановлення категорії інформації, що захищається; дослідження каналів витоку, модель загроз; модель порушника; комплекс організаційних та технічних заходів і засобів захисту інформації; структура КСЗІ; дослідження ефективності КСЗІ).

Тема 3. Комп'ютерні віруси та вірусологія.

Результати навчання – РН06, РН14.

Опис теми. Загальні відомості про комп'ютерні віруси: класифікація вірусів; алгоритми функціонування вірусів; технології та засоби створення і розповсюдження комп'ютерних вірусів. Технології захисту комп'ютерних систем від комп'ютерних вірусів: конструктори вірусів; антивірусне програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 3. Дослідження процесів захисту інформації від комп'ютерних вірусів: Створення ізольованого віртуального середовища досліджень; генерація вірусів та дослідження їх сигнатур; дослідження ефективності детектування сигнатур вірусів різними програмними засобами; створення системи захисту інформації від комп'ютерних вірусів та дослідження її ефективності.

Тема 4. Кібернетичні загрози комп'ютерним системам та протидія їм.

Результати навчання – РН06, РН14.

Опис теми. Методи і засоби реалізації кібернетичних атак: кібернетична та (і) комп'ютерна атака, поняття, класифікація, модель, зміст етапів; методи і технології організації та реалізації кібернетичних атак. Методи і засоби протидії кібернетичним атакам: методології, методи і технології протидії кібернетичним атакам (методи, програмне забезпечення та сутність його побудови і застосування); методи та технології захисту комп'ютерних систем від вірусів.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 4. Дослідження процесів захисту інформації від кібернетичних атак: Створення ізольованого віртуального середовища досліджень; дослідження уразливості оточення до кібернетичних впливів; створення системи захисту

інформації від кібернетичних впливів та дослідження її ефективності.

Тема 5. Криптографічний захист інформації в комп'ютерних системах.

Результати навчання – РН06, РН14.

Опис теми. Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз: Загальні відомості про шифрування, кодування, криптографію і криптологію; Задачі дешифрування; Технології та системи криптографічного захисту інформації. Традиційні історичні шифри. Математичні та алгоритмічні основи: Загальні відомості та галузі застосування. Шифрування на основі одно та багато алфавітних підстановок: шифри Цезаря та «скитала»; Шифр Віжинера та квадрати Уітстона. Біграмні шифри. Потокові шифри з необмеженою довжиною ключа. Шифрування «гамуванням». Традиційні історичні шифри. Технології реалізації та уразливість: Реалізація традиційних історичних шифрів з використанням засобів Python; Приклади реалізації традиційних шифрів в Python; Уразливість традиційних історичних шифрів.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 5. Дослідження технологій традиційного шифрування та їх уразливості: Розробка скрипта в Python, що реалізує технології традиційного шифрування за заданим алгоритмом та дослідження їх уразливості.

Тема 6. Методи, моделі, алгоритми та системи блочного шифрування.

Результати навчання – РН11, РН14.

Опис теми. Алгоритми блочного шифрування. Математичні та алгоритмічні основи: Сутність та математичні основи методів блочного шифрування. Алгоритми блочного шифрування. Технології реалізації та уразливість: Технології блочного шифрування в Python, уразливість.

Лекція – 4 год.

Лабораторна робота – 4 год.

Лабораторна робота № 6. Дослідження технологій блочного шифрування та їх уразливості: Розробка скрипта в Python, що реалізує технології блочного шифрування за заданим алгоритмом та дослідження їх уразливості.

Тема 7. Методи, моделі, алгоритми та системи симетричного шифрування.

Результати навчання – РН11, РН14.

Опис теми. Симетричні шифри та системи. Математичні та алгоритмічні основи: Шифрування на основі чередування перестановок та підстановок; Стандарт шифрування Data Encryption Standard. (DES). Симетричні шифри та системи. Технології реалізації та уразливість: Блок управління ключами в DES. Алгоритм 3-DES та чотири режими реалізації

криптографічного захисту на основі DES. Технології асиметричного шифрування в Python, уразливість.

Лекція – 4 год.

Лабораторна робота – 4 год.

Лабораторна робота № 7. Дослідження технологій симетричного шифрування та їх уразливості: Розробка скрипта в Python, що реалізує технології симетричного шифрування за заданим алгоритмом та дослідження їх уразливості.

Тема 8. Методи, моделі, алгоритми та системи асиметричного шифрування.

Результати навчання – РН05, РН14.

Опис теми. Асиметричні шифри та системи. Математичні та алгоритмічні основи: Криптографія по Діффі і Хелману. Незворотні функції в шифруванні. Три схеми та задачі криптозахисту. Система RSA. Модулярна арифметика. Алгоритм швидкого дискретного потенціювання. Процесор – акселератор RSA; Технології асиметричного шифрування в Python, уразливість. Тема 16. Асиметричні шифри та системи. Технології реалізації та уразливість: Проблема генерації великих простих чисел (ВПЧ). Тест Рабіна та мала теорема Ферма. Перевірки на простоту. Схеми та алгоритми розрахунків ключів для системи RSA. Класичний та розширений алгоритми Евкліда. Технології асиметричного шифрування в Python, уразливість.

Лекція – 4 год.

Лабораторна робота – 4 год.

Лабораторна робота № 8. Дослідження технологій асиметричного шифрування та їх уразливості: Розробка скрипта в Python, що реалізує технології асиметричного шифрування за заданим алгоритмом та дослідження їх уразливості.

Тема 9. Методи, методології, технології і засоби аутентифікації та ідентифікації.

Результати навчання – РН05, РН14.

Опис теми. Методи і технології ідентифікації користувачів в розподіленнях комп’ютерних системах: методи аутентифікація та ідентифікація суб’єктів на основі симетричних систем шифрування. Поняття майстер ключа та змінного ключа; технології аутентифікація та ідентифікація в Python.

Лекція – 4 год.

Лабораторна робота – 4 год.

Лабораторна робота № 9. Дослідження технологій аутентифікації та ідентифікації в розподілених комп’ютерних системах: Розробка скрипта в Python, що реалізує технології електронного цифрового підпису та дослідження ефективності процесів аутентифікації та ідентифікації в розподілених комп’ютерних системах.

Тема 10. Електронний цифровий підпис, методи та засоби.

Результати навчання – РН05, РН14.

Опис теми. Встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування. Поняття

сигнатури повідомлення та цифрового підпису; аутентифікація та ідентифікація суб'єктів в протоколах відкритих замовлень. Поняття електронних чеку та квитанції; багаторівнева організація формування та використання ключів шифрування. Функції майстер-ключа, системного, клієнтського, торгово-касового та сесійного ключів.

Лекція – 2 год.

Лабораторна робота – 2 год.

Лабораторна робота № 10. Аспекти кіберзахисту електронної документації та питання авторизації і ідентифікації об'єктівт а суб'єктів процесу.

Форми та методи навчання

Використовуються такі форми навчання: самостійна робота студентів, лабораторні заняття, лекційні заняття, що проводяться з використанням проектора для демонстрації процесу дослідження стійкості інформаційних систем та програмного забезпечення.

Тематика лабораторних робіт розрахована, у тому числі, й на виконання завдань навчально-дослідного характеру з частково невизначеними умовами.

Програма освітньої компоненти передбачає комплексне навчання вивчення засобів та заходів захисту інформаційних систем в усіх її аспектах з формуванням визначених в освітній програмі фахових компетентностей бакалавра з інформаційних систем та технологій.

Інструменти, обладнання, програмне забезпечення

Курс передбачає використання: консольних команд середовища windwows та unix/linux; програм: SIEM software,; а також засобів програмування середовища python.

Порядок оцінювання програмних результатів навчання/ результатів навчання

Для поточного контролю знань студентів з навчальної дисципліни використовуються такі методи:

- *на лабораторних заняттях проводиться контроль готовності до заняття шляхом тестового експрес-опитування, а також шляхом захисту звітів з лабораторної роботи у вигляді співбесіди;*
- *контроль самостійної роботи проводиться у вигляді співбесіди на задану тему;*
- *оцінка модульних контрольних робіт (тестування);*

Підсумковий контроль проводиться в кінці семестру у вигляді екзамену.

Усі форми контролю включено до 100-бальної шкали оцінювання.

Оцінювання результатів поточної роботи (завдань, що виконуються на лабораторних заняттях, результати самостійної роботи студентів) проводиться за такими критеріями:

Лабораторні роботи (у балах, виділених на завдання із заокругленням до цілого числа):

0 балів – завдання не виконано;

2 бали – завдання виконано частково та містить суттєві помилки методичного або розрахункового характеру;

3 бали – завдання виконано повністю, але містить суттєві помилки у розрахунках або в методиці;

4 бали – завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки (розмірності, висновки, оформлення тощо);

5 балів – завдання виконано правильно, вчасно і без зауважень.

Модульний контроль проходитиме у формі тестування. У тесті 27 запитань різної складності: рівень 1 – 24 запитань по 0,5 бали (12 балів), рівень 2 – 2 запитань по 2 бали (4 бали), рівень 3 – 1 запитання по 4 бали (4 бали). Усього – 20 балів.

Допуск до екзамену:

- *усі лабораторні роботи відроблені;*
- *виконання двох модульних контрольних робіт;*

Результати поточного семестрового контролю оцінюються за шкалою [0...60] балів. За підсумковий контроль у вигляді екзамену, студент може отримати [0...40] балів. У такому випадку до набраних під час екзамену балів додаються бали поточного контролю.

Нормативні документи: Навчально-науковий центр незалежного оцінювання | (nuwm.edu.ua).

Рекомендована література (основна, допоміжна)

Основна література.

1. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.
2. М.В. Захарченко, В.Г. Кононович, В.И. Кільдішев, Д.В. Голев. «Інформаційна безпека інформаційно-комунікаційних систем: навчальний посібник. Лабораторний практикум. Частина 1. Комплекси засобів захисту інформації від НСД.». - 2011.
3. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.
1. Біленчук П. Д., Обіход Т. В. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму. Часопис Київського університету права. 2018. № 3. С. 235–239. URL: http://nbuv.gov.ua/UJRN/Chkup_2018_3_54
2. Білявська Ю., Микитенко Н, Шестак Я. Кібербезпека та захист інформації під час пандемії COVID-19. Товари і ринки. 2021. №1. С. 34–46. URL: http://nbuv.gov.ua/UJRN/tovary_2021_1_5
3. Бойко В. Д., Василенко М. Д., Кухаренко С. В. Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення. Інформаційна безпека людини, суспільства, держави. 2019. № 3. С. 57–69. URL: http://nbuv.gov.ua/UJRN/iblsd_2019_3_8
4. Бурячок В. Л. Інформаційна та кібезбезпека: соціотехнічний аспект. Львів : Магнолія – 2006, 2018. 320 с.
5. Горлинський В., Горлинський Б. Кібербезпека як складова інформаційної безпеки України. Information Technology and Security. 2019. Vol. 7, Iss. 2. С. 136–148. URL: http://nbuv.gov.ua/UJRN/inftech_2019_7_2_5
6. Даник Ю. Г. Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони : підручник. Вид. 2-ге, перероб. та доп. Одеса.: ОНАЗ ім. О. С. Попова, 2019. 320 с.

Допоміжна література.

1. URL: ISO/IEC 15408-1:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model.
2. URL: ISO/IEC WD 15408-2 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components.
3. URL: ISO/IEC 15408-3:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components
4. Хорошко В. А. Методи та засоби захисту інформації. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с.
5. Безпека інформаційно-коммунікаційних систем. К. : Видавнича група BHV, 2009. – 608 с. Askoxylakis I., Ioannidis S., Katsikas S.K., Meadows C. (eds.) Computer Security - ESORICS 2016, Part I.

Інформаційні ресурси в Інтернет

1. URL: Національна бібліотека України імені В. І. Вернадського (nbuv.gov.ua)
2. URL: Рівненська обласна універсальна наукова бібліотека (libr.rv.ua)
3. URL: Рівненська централізована бібліотечна система (rivnecbs.com.ua)
4. URL: Бібліотека НУВГП (nuwm.edu.ua)

Поєднання навчання та досліджень

Студенти мають можливість додатково отримати бали за виконання індивідуальних завдань дослідницького характеру, а також можуть бути долучені до написання та опублікування наукових статей з тематики курсу.

Кожен здобувач вищої освіти може залучатися до написання та реалізації наукових робіт, статей, тез, патентів, проектів та інших робіт всеукраїнських та міжнародних досліджень.

ПОЛІТИКИ ВИКЛАДАННЯ ТА НАВЧАННЯ

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

Здатність застосовувати знання у практичних ситуаціях.

Здатність спілкуватися державною мовою як усно, так і письмово

Здатність працювати в команді.

Формування та розвиток критичного та аналітичного мислення.

Дедлайни та перескладання

Ліквідація академічної заборгованості здійснюється згідно: Порядок ліквідації академічних заборгованостей у НУВГП | (nuwm.edu.ua). *Згідно цього документу і реалізується право студента на повторне вивчення дисципліни чи повторне навчання на курсі.*

Перездача модульних контролів здійснюється згідно з: Якість освіти | (nuwm.edu.ua).

Оголошення стосовно дедлайнів здачі та перездачі оприлюднюються на сторінці: MOODLE - НУВГП | (nuwm.edu.ua).

Неформальна та інформальна освіта (за потреби)

Здобувачі освіти мають право на перезарахування результатів навчання у неформальній та інформальній освіті не більше ніж 25% загальної кількості кредитів освітньої програми на семестр – Центр неформальної освіти | (nuwm.edu.ua).

Правила академічної доброчесності

За списування під час проведення модульного контролю чи підсумкового контролю, студент позбавляється подальшого права здавати матеріал і у нього виникає академічна заборгованість.

За списування під час виконання окремих завдань, студенту знижується оцінка у відповідності до ступеня порушення академічної доброчесності.

Документи стосовно академічної доброчесності (про плагіат, порядок здачі курсових робіт, кодекс честі студентів, документи Національного агентства стосовно доброчесності) наведені на сторінці ЯКІСТЬ ОСВІТИ сайту НУВГП – Академічна доброчесність | (nuwm.edu.ua).

Вимоги до відвідування

Санкції за пропуски пар не передбачені. Студент має можливість самостійно вивчити необхідний для здачі модульних контролів та лабораторних робіт матеріал, який в повному обсязі дублюється викладачем одночасно на платформі Moodle та/або у групі з даного предмету в месенджері Telegram.

У разі необхідності проведення консультації – викладач йде назустріч. Відвідування пари допускається із використанням власного ноутбука. Студенти не повинні порушувати дисципліну на парі. Для студентів, які знаходяться на індивідуальному плані навчання, надаються індивідуальні завдання.

Студент має право оформити індивідуальний графік навчання згідно з Положення про індивідуальний графік навчання студентів денної форми навчання Національного університету водного господарства та природокористування | (nuwm.edu.ua).

[a]Там лише вибіркові дисципліни (ВБ2.2, ВБ 2.1, ВБ3.2) Їх вказувати?

Автор
Доцент ОТ Борис КРУЛІКОВСЬКИЙ

Затверджено

Проректор з науково-педагогічної та навчальної роботи — Валерій СОРОКА

документ підписаний КЕП
Номер документа СИЛ №1262
Підписувач Сорока Валерій Степанович
Підписувач (дані КЕП):
Сертифікат 3FAA9288358EC003040000009B6C3700C8C2C100