НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Навчально-науковий інститут автоматики, кібернетики та обчислювальної техніки

04-04-20S

СИЛАБУС **SYLLABUS**	**Системи технічного захисту інформації** **Systems of technical protection of information**	
Шифр за ОП Code in Degree Programme	ПП.2.11	
Освітній рівень Level of Education	Другий (Магістерський) Second (Master's)	
Галузь знань Field of Knowledge	12	Інформаційні технології Information Technology
Спеціальність Field of Study	123	Комп'ютерна інженерія Computer Engineering
Освітня програма Degree Programme	Комп'ютерна інженерія Computer Engineering	

РІВНЕ – 2023

Силабус навчальної дисципліни Системи технічного захисту інформації для здобувачів вищої освіти ступеня «магістр», які навчаються за освітньо-професійною програмою Комп'ютерна інженерія, спеціальності 123 Комп'ютерна інженерія. Рівне. НУВГП. 2023. 14 стор.
ОП на сайті університету
Розробник силабусу: Назарук В.Д., к.т.н., старший викладач кафедри обчислювальної техніки
Силабус схвалений на засіданні кафедри ОТ
Протокол № 6 від "27" 04 2023 року
Завідувач кафедри: Круліковський Б.Б., к.т.н., доцент
Керівник (гарант) ОП: Круліковський Б.Б., к.т.н., доцент, завідувач кафедри обчислювальної техніки
Схвалено науково-методичною радою з якості ННІАКОТ
Протокол № 6 від "27" квітня 2023 року.
Голова науково-методичної ради з якості ННІ: Мартинюк П.М., д.т.н., професор, директор ННІ Навчально-наукового інституту автоматики, кібернетики та обчислювальної техніки.
Попередня версія силабусу (вказати шифр) _-_

ПРОГРАМА
навчальної дисципліни Системи технічного захисту інформації

ЗАГАЛЬНА ІНФОРМАЦІЯ

Ступінь вищої освіти	*магістр.*
Освітня програма	Комп'ютерна інженерія
Спеціальність	Комп'ютерна інженерія
Рік навчання, семестр	*Перший рік, Перший семестр*
Кількість кредитів	*4*
Лекції:	*20*
Лабораторні заняття:	*20*
Самостійна робота:	*80*
Курсова робота:	*-*
Форма навчання	*денна/заочна*
Форма підсумкового контролю	*екзамен*
Мова викладання	*державна*

ІНФОРМАЦІЯ ПРО РОЗРОБНИКА

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*
ORCID	0000-0003-3705-5155
Як комунікувати	https://exam.nuwm.edu.ua/course/view.php?id=4185 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 ОСВІТНІЙ КОМПОНЕНТ

Мета та завдання

Мета дисципліни полягає в отриманні здобувачами вищої освіти теоретичних знань та практичних навичок побудови захищених інформаційних систем на основі сучасних засобів технічного 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

Посилання на розміщення освітнього компонента на навчальній платформі Moodle, на платформі освітніх програм та їхніх освітніх компонентів

https://exam.nuwm.edu.ua/course/view.php?id=4185

Передумови вивчення*

(місце освітнього компоненту в структурно-логічній схемі)

На матеріалі даної дисципліни може ґрунтуватись вивчення освітньої компоненти "Менеджмент інформаційної безпеки".

Компетентності

ЗК 6. Здатність виявляти, ставити та вирішувати проблеми.

СК 10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їх компонентів.

Програмні результати навчання (ПРН). Результати навчання (РН)*
РН 4. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань.
РН 10. Здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії, аналізувати та оцінювати цю інформацію.

Структура та зміст освітнього компонента	
Тема 1. Поняття інформації. Загрози для інформації. Основні види технічних засобів розвідки.	
Кільк. годин: 2 год лекцій; 9 год. сам. роб.	**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.	**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.	**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.	**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.	**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; 6 год. лаб. роб.; 9 год.сам. роб.	**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.** Інсталяція та деінсталяція комплексу засобів захисту «Лоза-1» **Лаб. роб. 6.** Робота з функціоналом комплексу засобів захисту «Лоза-1» **Лаб. роб. 7.** 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. Основні вимоги до криптографічних систем. Поняття криптоалгоритму. Симетричні криптоалгоритми	
Кільк. годин: 2 год лекцій; 2 год. лаб. роб.; 9 год.сам. роб	**Лекція 7.** 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. 8.** Математичне забезпечення симетричних криптоалгоритмів**.** **Сам. роб.** Симетричні криптоалгоритми докомп'ютерного періоду
Тема 8. Мережа Фейстеля. Криптоалгоритм DES	
Кільк. годин: 2 год лекцій; 4 год.сам. роб	**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: 2 год лекцій; 4 год.сам. роб	**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: 2 год лекцій; 4 год. лаб. роб.; 9 год.сам. роб	**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. 9** Генерація спільного закритого ключа для симетричного шифрування за алгоритмом Діффі-Хелмана **Лаб. роб. 10** Розрахунок параметрів відкритого та закритого ключа асиметричного криптоалгоритму RSA. Шифрування та розшифрування

	повідомлення за допомогою розрахованих параметрів. **Сам. роб.** Асиметричні криптоалгоритми на еліптичних кривих

Форми та методи навчання

- проблемні лекції;
- публічний виступ (презентація лекційного матеріалу, есе та захист завдань здобувачами);
- розгляд конкретних ситуацій;
- осліджeння сертифікованих в Україні комплексів засобів захисту;
- робота в малих групах та індивідуальні завдання;
- діалогові технології (дискусії, коментування, опонування тощо); рольове та імітаційне моделювання.

Інструменти, обладнання, програмне забезпечення

- Комп'ютерна аудиторія на 15 робочих місць з параметрами машин не нижче: Процесор - AMD Ryzen 3 5300G with Radeon Graphics 4.00 GHz, ОЗП - 8,00 ГБ;
- Операційна система Windows 10;
- Віртуальна машина Hyper-V;
- Комплекс засобів захисту «Лоза-1»;
- ПЗ TESTS1;
- Селективний мікровольтметр STV 301-2 з комплектом феритових стержневих антен FSA-101;
- Прилад радіочастотного зашумлення «Ріас-1М»;
- Токени авторизації Kingston 128 ГБ USB 3.2;
- Навчальна платформа Moodle.

Порядок оцінювання програмних результатів навчання/ результатів навчання

За поточну (практичну) складову оцінювання (1 лабораторна робота), балів	6
Усього за поточну (практичну) складову оцінювання, балів	60
За модульний (теоретичний) контроль знань (МК1, МК2) 20 балів	20
Усього за 2 модульні контроль, або екзамен, балів	40
Усього за дисципліну, балів	100

Методи оцінювання та структура оцінки *COURSE*	Для оцінювання рівня знань застосовується 100-бальна шкала оцінювання. Величина рівня засвоєння матеріалу навчання відбувається за такими методами:

GRADE COMPOSITION	• 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 (ЕК3 – до 40 балів). Модульні контролі та екзамен проводяться через ННЦНО НУВГП у формі комп'ютерного тестування на платформі Moodle. МК1, МК2 і ЕК3 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 (ЕК3);

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

Рекомендована література

Основна

1. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем К, «BHV», 2009. - 608с.
2. Тарнавський Ю. А. Технології захисту інформації: підручник Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
3. Хорошко В.О. Основи інформаційної безпеки: підручник В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест; за ред. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с
4. Поповский В.В., Персиков А.В. Основы криптографической защиты информации в телекоммуникационных системах Харьков: СМИТ 2010 465с.
4. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации . Том 1. Несанкционированное получение информации Киев: Арий 2008, 326с.

Допоміжна

1.Фергюсон Н., Шнайер Б. Практическая криптография. : Пер. с англ. — М.: Издательский дом "Вильямс", 2005. — 424 с. : ил.
2. Хорошков В. А., Чекатков А. А. Методы и средства защиты информации / Под ред. Ю. С. Ковтанюка – К.: Издательство Юниор, 2003.- 504с., ил.
3. 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.

Поєднання навчання та досліджень

Напрямок дослідження - проблеми впровадження комплексів захисту інформації в автоматизованих системах вітчизняними підприємствами, установами, організаціями.
Додаткові бали з дисципліни здобувачам зараховуються за участь в конференціях, круглих столах та семінарах, також за публікацію статей або тез доповідей за відповідною тематикою

ПОЛІТИКИ ВИКЛАДАННЯ ТА НАВЧАННЯ

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.

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 (за потреби)

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.

Лектор **Назарук Віталій Дмитрович**,
канд. техн. наук, ст. викладач кафедри обчислювальної техніки

Автор
Старший викладач Віталій НАЗАРУК

Затверджено

Проректор з науково-педагогічної та навчальної роботи Валерій СОРОКА

документ підписаний КЕП
Номер документа СИЛ №515 від [sDateTime_SignWriteAgree_Last]
Підписувач Сорока Валерій Степанович
Підписувач (дані КЕП): [oSignECP.sSigner_Sert]

Сертифікат 58E2D9E7F900307B04000000807E2D0054327D00