

Національний університет водного господарства та
природокористування
Навчально-науковий інститут автоматики, кібернетики та
обчислювальної техніки

ЗАТВЕРДЖУЮ

Голова науково-методичної
ради НУВГП
е-підпис Олег ЛАГОДНЮК

16.09.2021

04-01-48S

СИЛАБУС навчальної дисципліни		SYLLABUS	
Сучасні методи та технології захисту інформації		Modern methods and technologies of information protection	
Шифр за ОП	ВБ 2	Code in Educational Program	
Освітній рівень: магістерський (другий)		Educational level: Master's (second)	
Галузь знань: Інформаційні технології	12	Field of knowledge: Information technologies	
Спеціальність: Комп'ютерні науки	122	Field of study: Computer Science	
Освітня програма: Прикладна інформатика		Educational Program: Applied informatics	

Силабус навчальної дисципліни Сучасні методи та технології захисту інформації для здобувачів вищої освіти ступеня «магістр», які навчаються за освітньо-професійною програмою «Прикладна математика» спеціальності 122 «Комп'ютерні науки». Рівне. НУВГП. 2021. 20 стор.

ОПП на сайті університету: <http://ep3.nuwm.edu.ua/20987/>.

Розробник силабусу: Назарук Віталій Дмитрович, канд. техн. наук, старший викладач кафедри обчислювальної техніки

Силабус схвалений на засіданні кафедри комп'ютерних наук та прикладної математики

Протокол № 19 від "27" серпня 2021 року

Завідувач кафедри: Турбал Юрій Васильович, д.т.н., професор.

Схвалено науково-методичною радою з якості ННІ АКOT

Протокол № 9 від "30" серпня 2021 року

Голова науково-методичної ради з якості ННІ:

Мартинюк П. М., д-р техн., професор

СЗ №-4464 в ЕДО.

© Назарук В.Д., 2021

© НУВГП, 2021

ЗАГАЛЬНА ІНФОРМАЦІЯ*	
Ступінь вищої освіти	Магістр
Освітня програма	Прикладна інформатика
Спеціальність	122 «Комп'ютерні науки»
Рік навчання, семестр	1-й рік навчання, 2-й семестр
Кількість кредитів	4,5
Лекції:	20 год.
Лабораторні заняття:	26 год.
Самостійна робота:	89 год.
Курсова робота:	
Форма навчання	<i>Денна</i>
Форма підсумкового контролю	Залік
Мова викладання	Українська
ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА*	
ПРОФАЙЛ ЛЕКТОРА	
Лектор	<p>Назарук Віталій Дмитрович, канд. техн. наук, старший викладач кафедри обчислювальної техніки</p> <p>v.d.nazaruk@nuwm.edu.ua</p>
	
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	<p>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 Електронний 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</p>
ПРОФАЙЛ АСИСТЕНТА	

ПРО ДИСЦИПЛІНУ	
Анотація навчальної дисципліни, в т.ч. мета та цілі	<p>Навчальна дисципліна «Сучасні методи та технології захисту інформації» входить до циклу загальної підготовки студентів-магістрів зі спеціальності " Комп'ютерні науки" і є однією з ключових складових фундаментальної підготовки фахівців в галузі інформаційних технологій.</p> <p>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. Окремо надано основи менеджменту та аудиту інформаційної безпеки</p> <p>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.</p> <p>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</p>
Посилання на розміщення навчальної дисципліни на навчальній платформі Moodle	https://exam.nuwm.edu.ua/course/view.php?id=3019
Компетентності	<p>ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.</p> <p>ЗК2. Здатність застосовувати знання у</p>

	<p>практичних ситуаціях.</p> <p>ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.</p> <p>ЗК5. Здатність вчитися й оволодівати сучасними знаннями.</p> <p>ЗК6. Здатність бути критичним і самокритичним.</p> <p>ЗК7. Здатність генерувати нові ідеї (креативність).</p> <p>ЗК9. Здатність оцінювати та забезпечувати якість виконуваних робіт.</p> <p>ФК4. Здатність формалізувати предметну область певного проєкту у вигляді відповідної інформаційної моделі.</p> <p>ФК5. Здатність використовувати математичні методи для аналізу формалізованих моделей предметної області.</p> <p>ФК9. Здатність розробляти програмне забезпечення відповідно до сформульованих вимог з урахуванням наявних ресурсів та обмежень.</p> <p>ФК15. Здатність до оригінального мислення та проведення досліджень, критичне осмислення проблем у сфері комп'ютерних наук та на межі галузей знань.</p>
Програмні результати навчання	<p>ПРН1. Здійснювати опис предметної області розробки або дослідження; забезпечувати декомпозицію поставленої задачі.</p> <p>ПРН2. Обирати належні засоби для розробки або дослідження (середовище розробки, мова програмування, програмне забезпечення та програмні пакети тощо), що дозволяють знайти правильне і ефективне рішення.</p> <p>ПРН3. Аналізувати проміжні результати розробки або дослідження з метою з'ясування їх відповідності вимогам; розробляти тести та використовувати засоби верифікації, щоб переконатися у якості прийнятих рішень.</p> <p>ПРН7. Створювати прототипи програмного забезпечення, щоб переконатися, що воно відповідає вимогам до розробки; виконувати його тестування і статичний аналіз, щоб переконатися у відповідності завданню розробки або дослідження.</p> <p>ПРН9. Управляти складними робочими процесами з урахуванням поставлених</p>

	<p>економічних, правових та етичних аспектів, оцінювати результати діяльності команди.</p> <p>ПРН11. Відшукувати необхідну інформацію у науковій літературі, базах даних, інших джерелах, аналізувати і оцінювати її.</p> <p>ПРН13. Мати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері інформаційних технологій і є основою для оригінального мислення та проведення досліджень.</p>
Перелік соціальних, «м'яких» навичок (soft skills)	<ul style="list-style-type: none"> – 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 обговорення матеріалів навчання, перевірки результатів лабораторних робіт.

Структура навчальної дисципліни	
Лекції: 20 год.	Лабораторні роботи: 26 год.
Самостійна робота: 128 год.	
Результати навчання:	
РН1. Освоїти основні положення нормативно-правових документів із питань захисту інформації	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 1); самостійна робота з літературою; підготовка до контрольних заходів
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.

PH2. Освоїти основні вимоги вітчизняних нормативних документів із питань технічного захисту інформації	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 2); самостійна робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторної роботи № 1, лабораторної роботи № 2.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки, спеціалізоване обладнання для пошуку побічних електромагнітних випромінювань, спеціалізоване програмне забезпечення для створення тестових сигналів.
PH3. Освоїти основні вимоги міжнародних стандартів менеджменту інформаційної безпеки	
Види навчальної роботи	Вивчення лекційного матеріалу (тема 3); самостійна робота з літературою; підготовка до контрольних заходів.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки, спеціалізоване обладнання для пошуку побічних електромагнітних випромінювань, спеціалізоване програмне забезпечення для створення тестових сигналів, спеціалізоване обладнання для створення шипокосмугового електромагнітного шумового сигналу.
PH4. Освоїти основні вимоги міжнародних стандартів із аудиту системи менеджменту інформаційної безпеки	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 4); самостійна робота з літературою; підготовка до контрольних заходів.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання;

	навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки, нормативні документи із технічного захисту інформації
PH5. Оперувати основними функціями комплексів засобів захисту в автоматизованих системах від несанкціонованого доступу	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 5); самостійна робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторних робіт №№ 3, 4, 5, 6.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
PH6. Володіти основними поняттями симетричних криптоалгоритмів та вимогами до криптографічних систем	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 6); самостійна робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторної роботи № 7
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки, спеціалізоване програмне забезпечення «комплекс засобів захисту».
PH7. Володіти основними характеристиками алгоритмів мережі Фейстеля та криптоалгоритму DES	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 7); самостійна робота з літературою; підготовка до контрольних заходів.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання;

	навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
PH8. Володіти основними характеристиками асиметричних криптоалгоритмів, зокрема алгоритму Діффі-Хеллмана та криптоалгоритму RSA.	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 8); самостійна робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторних робіт №№ 8, 9, 10.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
PH9. Освоїти основними характеристиками сучасних ХЕШ-функцій. Володіти прийомами генерування, застосування та верифікації електронного цифрового підпису.	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 9); самостійна робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторної роботи № 11.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
PH10. Вміти локалізувати небезпечні сигнали побічних електромагнітних випромінювань на об'єктах інформаційної діяльності.	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 10); самостійна робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторних робіт №№ 12, 13.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання;

	навчання на основі досвіду).		
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.		
ЛЕКЦІЇ ТА ПРАКТИЧНІ РОБОТИ:			
Тема 1. План навчальної дисципліни. Нормативно-правові акти із питань захисту інформації			
Результати навчання: РН1	Кількість 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=3640
Опис теми:	<p>Лекція 1. План навчальної дисципліни. Законодавчі акти із питань захисту інформації.</p> <p><i>План навчальної дисципліни. Закон України Про захист інформації в інформаційно-телекомунікаційних системах. Закон України Про основні засади забезпечення кібербезпеки України. Закон України Про електронні довірчі послуги.</i></p> <p>Сам. роб. Основні вимоги Постанови КМУ від 29. 03. 2006 р. N 373 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.</p>		
Тема 2. Вимоги нормативних документів із технічного захисту інформації			
Результати навчання: РН3	Кількість годин: 2 год лекцій; 4 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=3640
Опис теми:	<p>Лекція 2. Вимоги нормативних документів із технічного захисту інформації.</p> <p><i>Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу,</i></p> <p>Лаб. роб. 1. Категоріювання об'єкта, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.</p> <p>Лаб. роб. 2. Підготовка вимог до захисту інформації веб-порталу університету.</p> <p>Сам. роб. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності.</p>		

Тема 3. Міжнародні стандарти з інформаційної безпеки. Основні положення та вимоги.			
Результати навчання: PH4	Кількість годин: 2 год лекцій; 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=3640
Опис теми:	<p>Лекція 3. Міжнародні стандарти з інформаційної безпеки. Основні положення та вимоги.</p> <p><i>Системи управління ІБ Стандарт ISO/IEC 27000-2017. Вимоги до системи управління інформаційною безпекою. (стандарт ISO / IEC 27001: 2018). Звід правил управління інформаційною безпекою (стандарт ISO / IEC 27002: 2013).</i></p> <p>Сам. роб. Розробка системи управління інформаційною безпекою. Визначення області дії, меж і політики СУІБ (стандарт ISO / IEC 27003: 2010). Управління ризиками інформаційної безпеки (Стандарт ISO / IEC 27005: 2010).</p>		
Тема 4. Аудит систем менеджменту інформаційної безпеки.			
Результати навчання: PH5	Кількість годин: 2 год лекцій; 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=3640
Опис теми:	<p>Лекція 4. Аудит систем менеджменту інформаційної безпеки. Аудит систем менеджменту інформаційної безпеки. Становлення процесу аудиту менеджменту інформаційної безпеки. Правові основи аудиту системи менеджменту інформаційної безпеки.</p> <p>Сам. роб. Аудит систем менеджменту інформаційної безпеки згідно міжнародних стандартів ISO 19011.</p>		
Тема 5. Комплекси засобів захисту для автоматизованих систем.			
	Кількість 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=3640
Опис теми:	<p>Лекція 5. Комплекси засобів захисту для автоматизованих систем.</p> <p><i>Функції комплексів засобів захисту. Функціональний профіль захищеності і рівень гарантій. Політики функціональних послуг безпеки. Монітор безпеки.</i></p> <p>Лаб. роб. 3. Вивчення функціональних характеристик комплексу засобів захисту «Лоза-1».</p> <p>Лаб. роб. 4. Інсталяція та деінсталяція комплексу засобів захисту «Лоза-1»</p> <p>Лаб. роб. 5. Робота з переліком користувачів комплексу засобів захисту «Лоза-1»</p> <p>Лаб. роб. 6. Робота з переліком користувачів системи «Лоза-1»</p> <p>Сам. роб. Функціонал адміністратора K33 та адміністратора</p>		

	безпеки комплексу засобів захисту від несанкціонованого доступу.		
За поточну (практичну) складову оцінювання 36 балів		За модульний (теоретичний) контроль знань (МК1) 20 балів	
Тема 6. Криптографічний захист інформації. Основні вимоги до криптографічних систем. Поняття криптоалгоритму. Симетричні криптоалгоритми			
Результати навчання: РН7	Кількість 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=3640
Опис теми:	<p>Лекція 6. Криптографічний захист інформації. Основні вимоги до криптографічних систем. Поняття криптоалгоритму <i>Історія криптології. Основні вимоги до криптосистем. Загальна схема симетричного шифрування. Методи заміни. Пропорційні шифри. Багатоалфавітна підстановки.</i></p> <p>Лаб. роб. 7. Основи криптографічного захисту інформації. Симетричні криптоалгоритми.</p> <p>Сам. роб. Симетричні криптоалгоритми докомп'ютерного періоду</p>		
Тема 7. Мережа Фейстеля. Криптоалгоритм DES			
Результати навчання: РН8	Кількість 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=3640
Опис теми:	<p>Лекція 7. Мережа Фейстеля. Криптоалгоритм DES <i>Вимоги до блокового криптоалгоритму. Алгоритм мережі Фейстеля. Криптоалгоритм DES – загальна схема, структура раунду.</i></p> <p>Сам. роб. Симетричні криптоалгоритми на основі мережі Фейстеля. Криптоалгоритм 28147-89</p>		
Тема 8. Асиметричні криптоалгоритми. Алгоритм Діффі-Хеллмана. Криптоалгоритм RSA. Основні відомості. Шифрування та розшифрування. Практичне використання			
Результати навчання: РН8	Кількість годин: 2 год лекцій; 6 год. лаб. роб 9 год. сам. роб	Література: 1, с.255-282; 2, с.375-394;	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640
Опис теми:	<p>Лекція 8 Асиметричні криптоалгоритми. Алгоритм Діффі-Хеллмана. Криптоалгоритм RSA. Основні відомості. Шифрування та розшифрування. Практичне використання <i>Алгоритм Діффі-Хеллмана - основні відомості, приклади обчислень, практичне використання. Криптоалгоритм RSA - основні відомості, приклади обчислень, практичне використання.</i></p> <p>Лаб. роб. 8 Генерація спільного закритого ключа для симетричного шифрування за алгоритмом Діффі-Хеллмана</p>		

<p>Лаб. роб. 9 Розрахунок параметрів відкритого та закритого ключа асиметричного криптоалгоритму RSA. Шифрування та розшифрування повідомлення за допомогою розрахованих параметрів.</p> <p>Лаб. роб. 10 Шифрування інформації за допомогою асиметричних криптоалгоритмів в програмному середовищі Gpg4win</p> <p>Сам. роб. Асиметричні криптоалгоритми на еліптичних кривих</p>			
<p>Тема 9. ХЕШ-функція. Електронний цифровий підпис.</p>			
Результати навчання: РН8	Кількість годин: 2 год лекцій; 2 год лаб. роб. 9 год. сам. роб.	Література: 1, с.284-325; 2, с.395-426;	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640
Опис теми:	<p>Лекція 9 ХЕШ-функція. Електронний цифровий підпис. <i>Алгоритми хешування. Застосування хеш-функцій. Хеш-функції сімейства MD. Електронний цифровий підпис. Акредитовані центри довірчих послуг</i></p> <p>Лаб. роб. 11. Генерація, застосування та верифікація кваліфікованого електронного підпису (КЕП)</p> <p>Сам. роб. Вивчення хеш-функції сімейства SHA</p>		
<p>Тема 10. Технічні каналів витоку інформації. Класифікація. Види. Модель технічного каналу витоку інформації.</p>			
Результати навчання: РН2	Кількість годин: 2 год лекцій; 4 год. лаб. роб.; 8 год. сам. роб.	Література: 1, с. 131-147;	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640
Опис теми:	<p>Лекція 10. Технічні каналів витоку інформації. Класифікація. Види. Модель технічного каналу витоку інформації. <i>Поняття технічного каналу витоку інформації. Класифікація ТКВІ. Небезпечні сигнали. Контрольована зона.</i></p> <p>Лаб. роб. 12. Визначення амплітуди гармонік та побудова спектра побічних електромагнітних випромінювань монітора комп'ютера.</p> <p>Лаб. роб. 13. Локалізація побічних електромагнітних випромінювань монітора комп'ютера.</p> <p>Сам. роб. Вивчення засобів та методів виявлення небезпечних сигналів на об'єктах інформаційної діяльності</p>		
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
<p>Методи оцінювання та структура оцінки <i>COURSE GRADE COMPOSITION</i></p>	<p>Для оцінювання рівня знань застосовується 100-бальна шкала оцінювання. Величина рівня засвоєння матеріалу навчання відбувається за такими методами:</p> <ul style="list-style-type: none"> • 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. <p>Основними показниками, що характеризують рівень знань студента за результатами вивчення дисципліни є:</p> <ul style="list-style-type: none"> • 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. <p>Оцінювання результатів роботи проводиться у % від кількості балів, виділених на завдання, із заокругленням до цілого числа:</p> <ul style="list-style-type: none"> 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. <p>Поточна (практична) складова оцінки (не більше, ніж 60 балів) нараховується за виконання лабораторних робіт (до 4 балів за кожну лабораторну роботу №№ 1 – 9, та по 6 балів за кожну лабораторну роботу №№ 10 – 13); виконання самостійної роботи (реферат, презентація – до 5 балів; виконання лабораторних робіт з програмною</p>

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 контролю 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 (ЕК3); за одне завдання третього рівня складності – до 4 балів (МК1 і МК2) або до 8 балів (ЕК3).

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 для екзамену
90–100	відмінно
82–89	добре
74–81	
64–73	задовільно
60–63	
0–59	незадовільно

Місце навчальної дисципліни в освітній траєкторії здобувача вищої освіти

Опанування основними положеннями дисципліни передбачає наявність попередніх знань з вищої математики, математичної логіки та теорії алгоритмів, комп'ютерних мереж, операційних систем.

Дисципліни, що вивчаються паралельно з цією:
 – Проектування інформаційних систем

	<p>– Технології розподілених систем та паралельних обчислень</p> <p>Дисципліни, для вивчення яких обов'язкові знання даної навчальної дисципліни:</p> <p>– Проектування інформаційних систем</p> <p>– Технології тестування програмних продуктів/ Моделювання систем</p>
Інформаційні ресурси	<p style="text-align: center;">Рекомендована література</p> <p style="text-align: center;">Основна</p> <ol style="list-style-type: none"> 1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации . Том 1. Несанкционированное получение информации Киев: Арий 2008, 326с. 2. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации . Том 2. Информационная безопасность Ки-ев: Арий 2008 385с. 3. Поповский В.В., Персиков А.В. Основы криптографической защиты информации в телекоммуникационных системах Харьков: СМІТ 2010 465с. 4. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем К, «ВНУ», 2009. - 608с. 5. Бирюков И.В. Информационная безопасность. Защита и нападение : М, ДМК, 2017 - 434 с. <p style="text-align: center;">Допоміжна</p> <ol style="list-style-type: none"> 1. Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997.- 368с.:ил. 2. Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369 (Перевод В.Ф.Писаренко) 3. Козлов Д. А., Парандовский А. А., Парандовский А. К. Энцикло-педия компьютерных вирусов. - М.: «СОЛОН-Р», 2001. 4. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина.-2-е изд., перераб. и доп.-М.: Радио и связь, 2001.-376 с: ил. 5. Фергюсон Н., Шнайер Б. Практическая криптография. : Пер. с англ. — М.: Издательский дом "Вильямс", 2005. — 424 с. : ил. 6. Хорошков В. А., Чекатков А. А. Методы и средства

	<p>защиты информации / Под ред. Ю. С. Ковтанюка – К.: Издательство Юниор, 2003.- 504с., ил.</p> <p>7. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. - М.: "Триумф", 2002.</p> <p style="text-align: center;">Додаткові інформаційні ресурси</p> <p>1. Національна бібліотека ім. В. І. Вернадського. URL: http://www.nbuv.gov.ua/e-resources/, http://www.nbuv.gov.ua/webnavigator/</p> <p>2. Рівненська обласна універсальна наукова бібліотека (м. Рівне, майдан Короленка, 6). URL: http://www.lib.rv.ua/</p> <p>3. Рівненська централізована бібліотечна система (м. Рівне, вул. Київська, 44). URL: http://cbs.rv.ua/</p> <p>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</p> <p>5. Цифровий репозиторій НУВГП. URL: http://ep3.nuwm.edu.ua.</p> <p>6. Нормативні документи з питань технічного захисту інформації https://cip.gov.ua/ua/news/perelik-dokumentiv-sistemi-tekhnichnogo-zakhistu-informaciyi-nd-tzi</p>
ПРАВИЛА ТА ВИМОГИ (ПОЛІТИКА)	
Дедлайни та перескладання	<p>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%.</p> <p>Кінцевим терміном здачі завдань є останній робочий день навчального семестру (25 травня 2021 р.)</p> <p>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/.</p> <p>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-nezaleznoho-otsiniuvannia-znan/dokumenty.</p> <p>Перша перездача проводиться через ННЦНО згідно з розкладом перездач, який розміщено в додатку Мій НУВГП та ПС-Студент WEB:</p>

	<p>http://desk.nuwm.edu.ua/cgi-bin/shell.cgi?n=999.</p> <p>У випадку отримання незадовільної оцінки, здобувач направляє 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.</p> <p>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.</p>
<p>Правила академічної доброчесності</p>	<p>Викладач та здобувачі несуть спільну відповідальність за створення сприятливого творчого навчального середовища, яке базується на взаємній повазі.</p> <p>До кожного заняття здобувачі повинні наперед ознайомитися з матеріалами та інформаційними ресурсами, наведеними у методичних вказівках і розміщеними на сторінці дисципліни в Moodle.</p> <p>Здобувачі освіти повинні дотримуватися Кодексу честі студентів. http://nuwm.edu.ua/strukturni-pidrozdzili/vvrsdev/dokumenty</p> <p>Принцип студентоцентризму передбачає розуміння серйозності ставлення до академічної недоброчесності та неправомірної поведінки.</p> <p>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 прийнятної привади для плагіату чи обману.</p> <p>Здобувачі освіти не можуть копіювати виконані завдання у інших студентів, ділитися виконаними завданнями з іншими студентами і мають</p>

	<p>дотримуватися Положення про виявлення та запобігання академічного плагіату в НУВГП http://nuwm.edu.ua/sp/akademichna-dobrochesnistj</p> <p>У випадку плагіату при виконанні завдання здобувач не отримує бали і повинен виконати завдання повторно.</p> <p>Перевірка дотримання доброчесності під час модульного та підсумкового контролю може здійснюватися засобами відеонагляду.</p> <p>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.</p>
<p>Вимоги до відвідування</p>	<p>Здобувачі вищої освіти зобов'язані відвідувати усі лекційні та практичні заняття з дисципліни згідно розкладу http://desk.nuwm.edu.ua/cgi-bin/timetable.cgi</p> <p>Відвідування консультацій не обов'язкове.</p> <p>У випадку відсутності з поважних причин (індивідуальний план, лікарняний, мобільність тощо) здобувач самостійно опрацьовує теоретичний матеріал і виконує завдання з відповідної практичної роботи.</p> <p>Завдання до практичних робіт розміщено на платформі Moodle https://exam.nuwm.edu.ua/course/view.php?id=1818</p> <p>Файл (файли) із виконаними розрахунками здобувач прикріплює до відповідних завдань на платформі Moodle. Захист роботи відбувається на наступному занятті, консультації або онлайн у відеорежимі.</p> <p>На лекціях і практичних заняттях студенти можуть використовувати свої ноутбуки, планшети чи смартфони для роботи.</p>
<p>Неформальна та інформальна освіта</p>	<p>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</p> <p>Здобувачі можуть пройти відкриті онлайн курси, близькі за темою до даної навчальної дисципліни, таких платформ як Coursera, Prometheus, edEx, edEra, VUMOnline, FutureLearn тощо.</p> <p>Зокрема, рекомендується курс на платформі</p>

	<p>Coursera: Cybersecurity Compliance Framework & System Administration https://www.coursera.org/learn/cybersecurity-compliance-framework-system-administration</p>
ДОДАТКОВО	
Правила отримання зворотної інформації про дисципліну	<p>Здобувач має право звертатися до викладача за додатковим поясненням матеріалу теми, змісту завдань практичних робіт та самостійної роботи протягом семестру усно (під час занять чи консультацій), корпоративною електронною поштою або через систему повідомлень Moodle.</p> <p>Консультації можуть проводитися онлайн із застосуванням сервісу Google Hangouts Meet.</p> <p>Здобувачі вищої освіти можуть подавати свої критичні зауваження, а також ідеї та рекомендації щодо наповнення навчальної дисципліни і методів викладання шляхом анонімного онлайн анкетування через Google Forms, яке проводиться наприкінці кожного семестру.</p> <p>Незалежне оцінювання якості викладання проводиться Відділом якості освіти. http://nuwm.edu.ua/struktturni-pidrozdili/vyo/dokumenty</p>
Оновлення	<p>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.</p>
Навчання осіб з інвалідністю	<p>Навчання людей з інвалідністю проводиться за дотриманням вимог нормативних документів, розроблених в НУВГП: http://nuwm.edu.ua/sp/dlja-osib-z-invalidnistju</p> <p>До здобувачів вищої освіти з особливими потребами є прохання: завчасно повідомити лектора про вказані особливості для відповідної підготовки та їх врахування в організації навчального процесу.</p>
Інтернаціоналізація	<p>Програма національних обмінів «Плацкарт» відповідно до Положення http://ep3.nuwm.edu.ua/13963/ .</p> <p>За угодами про міжнародну академічну мобільність (Еразмус+ K1), на основі двосторонніх договорів між НУВГП та зарубіжними навчальними закладами.</p>
Лектор	Назарук Віталій Дмитрович,

	канд. техн. наук, ст. викладач кафедри обчислювальної техніки
--	--