НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Навчально-науковий інститут автоматики, кібернетики та обчислювальної техніки

04-04-21S

СИЛАБУС **SYLLABUS**	**Менеджмент інформаційної безпеки** **Management of information security**	
Шифр за ОП Code in Degree Programme	ПП.2.12	
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 Менеджмент інформаційної безпеки для здобувачів вищої освіти ступеня «магістр», які

навчаються за освітньо-професійною програмою Комп'ютерна інженерія, спеціальності 123 Комп'ютерна інженерія. Рівне. НУВГП. 2023. 16 стор.

ОП на сайті університету

Розробник силабусу: Назарук В.Д., к.т.н., старший викладач кафедри обчислювальної техніки

Силабус схвалений на засіданні кафедри
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 ННІ
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 Менеджмент інформаційної безпеки

ЗАГАЛЬНА ІНФОРМАЦІЯ

Ступінь вищої освіти	*магістр.*
Освітня програма	Комп'ютерна інженерія
Спеціальність	Комп'ютерна інженерія
Рік навчання, семестр	*Перший рік, другий семестр*
Кількість кредитів	*6*
Лекції:	*30*
Лабораторні заняття:	*30*
Самостійна робота:	*120*
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	https://orcid.org/0000-0003-3705-5155
Як комунікувати	https://exam.nuwm.edu.ua/course/view.php?id=4526 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 знань та вмінь з теорії та практики побудови систем управління інформаційною безпекою в організаціях, установах, підприємствах. Отримання ґрунтовних знань для впровадження програми аудиту системи менеджменту інформаційної безпеки, аналізу досягнення цілей аудиту та можливості для її вдосконалення..

Основними завданнями є формування навичок аналізу систем менеджменту інформаційної безпеки з метою впровадження їх в організаціях з дотриманням вимог прийнятих національних та міжнародних стандартів; набуття студентами теоретичних знань та практичних навичок щодо управління інформаційною безпекою в інформаційно-телекомунікаційних (автоматизованих) системах для реалізації встановленої політики безпеки; отримання фахових компетентностей для здійснення планування та проведення аудитів систем менеджменту інформаційної безпеки.

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=4526

Передумови вивчення*

(місце освітнього компоненту в структурно-логічній схемі)

На матеріалі даної дисципліни ґрунтується вивчення освітньої компоненти "Системи технічного захисту інформації".

Компетентності

ЗК 6. Здатність виявляти, ставити та вирішувати проблеми.

ЗК 7. Здатність приймати обґрунтовані рішення.

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

СК 11. Здатність обирати ефективні методи розв’язування складних задач комп’ютерної інженерії, критично оцінювати отримані результати та аргументувати прийняті рішення.

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

РН 2. Знаходити необхідні дані, аналізувати та оцінювати їх.

РН8 Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп’ютерних систем та мереж для вирішення складних задач комп’ютерної інженерії та дотичних проблем.

РН 10. Здійснювати пошук інформації в різних джерелах для розв’язання задач комп’ютерної інженерії, аналізувати та оцінювати цю інформацію.

РН 11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп’ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

Структура та зміст освітнього компонента

Тема 1. Об'єкти інформаційної безпеки. Основні складові інформаційної безпеки..

Кільк. годин: 2 год лекцій; 2 год. лаб. роб.; 9 год.сам. роб.	**Лекція 1.** План навчальної дисципліни «Менеджмент інформаційної безпеки». Об'єкти інформаційної безпеки. Основні складові інформаційної безпеки. *План навчальної дисципліни «Менеджмент інформаційної безпеки». Об'єкти інформаційної безпеки. Основні складові інформаційної безпеки. Необхідність управління інформаційною безпекою. Важливість і складність проблем інформаційної безпеки* **Лаб. роб. 1.** Об'єкти інформаційної безпеки. Основні складові інформаційної безпеки. **Сам. роб.** Вивчення Постанови Кабінету Міністрів України від 08 жовтня 1997 року № 1126 "Про затвердження Концепції технічного захисту інформації в Україні".

Тема 2. Роль стандартів в сфері інформаційної безпеки. Критерії оцінки довірених комп'ютерних систем.

Кільк. годин:	**Лекція 2.** Роль стандартів в сфері ІБ. Критерії

2 год лекцій; 2 год. лаб. роб.; 9 год.сам. роб.	оцінки довірених комп'ютерних систем *Роль стандартів в сфері ІБ. Критерії оцінки довірених комп'ютерних систем – «Помаранчева книга» (TCSEC). Основні характеристики* **Лаб. роб. 2.** Дослідження основних положень «Критеріїв оцінки довірених комп'ютерних систем» (Trusted Computer System Evaluation Criteria, TCSEC). Частина 1. **Сам. роб.** Вивчення Постанови Кабінету Міністрів України від 29 березня 2006 року № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах"
Тема 3. Основні поняття і принципи оцінки безпеки ІТ. Загальні критерії - ISO / IEC 15408.	
Кільк. годин: 2 год лекцій; 2 год. лаб. роб.; 9 год.сам. роб.	**Лекція 3.** Основні поняття і принципи оцінки безпеки ІТ. Загальні критерії - ISO / IEC 15408.. *Історія створення Загальних критеріїв. Структура та основні положення стандарту ISO / IEC 15408.Оцінка характеристик безпеки продуктів і систем ІТ згідно вимог стандарту* **Лаб. роб. 3.** Дослідження основних положень «Критеріїв оцінки довірених комп'ютерних систем» (Trusted Computer System Evaluation Criteria, TCSEC). Частина 1. **Сам. роб.** Вивчення Указу Президента України від 27 вересня 1999 року № 1229 "Про затвердження Положення про технічний захист інформації в Україні".
Тема 4. Розвиток і становлення стандартів управління інформаційною безпекою. Стандарт ISO/IEC 27000-2017.	
Кільк. годин: 2 год лекцій; 2 год. лаб. роб.; 9 год.сам. роб.	**Лекція 4.** Історія розвитку стандартів управління ІБ Стандарт ISO/IEC 27000-2017 *Історія розвитку стандартів управління ІБ в Європі. Стандарт ISO/IEC 27000-2017. Основні характеристики.* **Лаб. роб. 4.** Дослідження положень міжнародного стандарту ДСТУ ISO / IEC 15408-1-2017 «Критерії оцінки безпеки інформаційної технології. Частина 1. Вступ та загальна модель». Частина 1 **Сам. роб.** Вивчення Наказу Адміністрації Держспецзв'язку від 26 березня 2007 року № 45 "Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації".
Тема 5. Системи управління інформаційною безпекою. Сертифікація Систем управління інформаційною безпекою. Стандарт ISO/IEC	

27005-2017.	
Кільк. годин: 2 год лекцій; 2 год. лаб. роб.; 9 год.сам. роб.	**Лекція 5.** Системи управління ІБ. Сертифікація СУІБ. Стандарт ISO/IEC 27005-2017. *Впровадження, контроль, супровід і поліпшення СУІБ. Оцінка та обробка ризиків. Вибір і впровадження засобів захисту. Вирішальні фактори успіху СУІБ.* **Лаб. роб. 5** Дослідження положень міжнародного стандарту ДСТУ ISO / IEC 15408-1-2017 «Критерії оцінки безпеки інформаційної технології. Частина 1. Вступ та загальна модель». Частина 2. **Сам. роб.** Вивчення положень Нормативного документу системи технічного захисту інформації НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу".
Тема 6. Вимоги до системи управління інформаційною безпекою.	
Кільк. годин: 2 год лекцій; 2 год. лаб. роб.; 9 год.сам. роб.	**Лекція 6.** Вимоги до системи управління інформаційною безпекою згідно стандарту ISO / IEC 27001: 2018). *Сфера застосування. Контекст організації. Лідерство. Планування. Підтримка. Експлуатація. Оцінка результативності.* **Лаб. роб. 6.** Дослідження положень міжнародного стандарту ISO/IEC 27000-2016. «Інформаційні технології. Система управління інформаційною безпекою. Загальний огляд і термінологія». **Сам. роб.** Вивчення положень Нормативного документу системи технічного захисту інформації НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу".
Тема 7. Звід правил управління інформаційною безпекою	
Кільк. годин: 10 год лекцій; 8 год. лаб. роб.; 30 год.сам. роб	**Лекція 7.** Звід правил управління інформаційною безпекою (стандарт ISO / IEC 27002: 2013) Політика ІБ. Організація ІБ *Керівні положення для ІБ. Організація ІБ. Безпека, пов'язана з персоналом.* **Лекція 8.** Звід правил управління інформаційною безпекою (стандарт ISO / IEC 27002: 2013). Управління активами. Управління доступом. *Управління активами. Відповідальність за активи Безпека активів. Управління доступом.* **Лекція 9.** Звід правил управління інформаційною безпекою (стандарт ISO / IEC 27002: 2013). Управління доступом до системи і додатків. Криптографія. Фізична і екологічна безпека. *Управління доступом до системи і додатків. Криптографія. Фізична і екологічна безпека.* **Лекція 10.** Звід правил управління інформаційною безпекою (стандарт ISO / IEC 27002: 2013). Безпека операцій. Безпека зв'язку.

	Операційні процедури. Управління змінами. Поділ середовищ розробки, тестування та експлуатації. Контроль системного ПЗ. Захист від шкідливого ПЗ. Управління мережевою безпекою. **Лекція 11.** Звід правил управління інформаційною безпекою (стандарт ISO / IEC 27002: 2013). Передача інформації. Купівля, розробка та супроводження ІС. *Політики передачі інформації. Угода про нерозголошення. ІБ сервісів в загальнодоступних мережах. ІБ при розробці ІС.* **Лаб. роб. 7.** Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27001:2015. «Методи захисту. Системи управління інформаційною безпекою. Вимоги»**.** **Лаб. роб. 8.** Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27002:2015. «Методи захисту. Звід практик щодо заходів інформаційної безпеки.» **Лаб. роб. 9.** Дослідження положень міжнародного стандарту ISO/IEC 27011 МСЕ-Т РЕКОМЕНДАЦІЯ X.1051 Інформаційні технології - Методи безпеки - Настанови щодо управління інформаційною безпекою для телекомунікаційних організацій на основі ISO/IEC 27002 **Лаб. роб. 10.** Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27004:2018. «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання»**.** **Сам. роб.** Вивчення положень Нормативних документів системи технічного захисту інформації НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі", НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".
Тема 8. Розробка системи управління інформаційною безпекою. (стандарт ISO / IEC 27003: 2010)	
Кільк. годин: 2 год лекцій; 9 год.сам. роб	**Лекція 12.** Розробка системи управління інформаційною безпекою. Визначення області дії, меж і політики СУІБ (стандарт ISO / IEC 27003: 2010) *Отримання схвалення керівництва для проектування СУІБ. Визначення області дії і політики СУІБ. Проведення аналізу організації. Проведення аналізу та планування обробки ризиків. Розробка СУІБ.* **Лаб. роб. 11.** Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27003:2018. «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанови» (Частина 1).

	Лаб. роб. 12. Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27003:2018. «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанови» (Частина 2)**.** **Сам. роб.** Вивчення положень Нормативного документу системи технічного захисту інформації НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу".
Тема 9. Управління ризиками інформаційної безпеки. Основні критерії	
Кільк. годин: 2 год лекцій; 2 год. лаб. роб.; 9 год.сам. роб	**Лекція 13.** Управління ризиками інформаційної безпеки (Стандарт ISO / IEC 27005: 2010). Основні критерії *Ідентифікації ризиків. Оцінка ризиків. Вивчення потенційних наслідків ризиків. Встановлення порядку пріоритетів в рамках обробки ризиків. Заходи щодо зниження ризиків.* **Лаб. роб. 13** Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27005:2015. «Методи захисту. Управління ризиками інформаційної безпеки» **Сам. роб.** Вивчення положень Нормативного документу системи технічного захисту інформації НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі".
Тема 10. Управління ризиками інформаційної безпеки. Оцінка наслідків інцидентів. Обробка ризиків. (Стандарт ISO / IEC 27005: 2010).	
Кільк. годин: 2 год лекцій; 2 год. лаб. роб.; 9 год.сам. роб	**Лекція 14** Управління ризиками інформаційної безпеки. Оцінка наслідків інцидентів. Обробка ризиків (Стандарт ISO / IEC 27005: 2010)ф *Оцінка наслідків інциденту. Обробка ризиків ІБ.* **Лаб. роб. 14** Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27007:2018. «Інформаційні технології. Методи захисту. Настанови щодо аудиту систем керування інформаційною безпекою». **Сам. роб.** Вивчення положень Нормативного документу системи технічного захисту інформації НД ТЗІ 2.5-008-2002 "Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2"

Тема 10. Аудит систем менеджменту інформаційної безпеки.

Кільк. годин: 2 год лекцій; 2 год. лаб. роб.; 9 год.сам. роб	**Лекція 15** Аудит систем менеджменту інформаційної безпеки. Правові основи та види аудиту системи менеджменту інформаційної безпеки *Правові основи аудиту системи менеджменту інформаційної безпеки. Види аудиту систем менеджменту інформаційної безпеки* **Лаб. роб. 9** Підготовка програми аудиту системи менеджменту інформаційної безпеки організації за вимогами стандарту ISO 19011-2011. **Сам. роб.** Вивчення положень Нормативного документу системи технічного захисту інформації НД ТЗІ 2.5-010-2003 "Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу"

Форми та методи навчання

- проблемні лекції;
- публічний виступ (презентація лекційного матеріалу, есе та захист завдань здобувачами);
- розгляд конкретних ситуацій;
- аналіз менеджменту інформаційної безпеки реальних підприємств;
- робота в малих групах та індивідуальні завдання;
- діалогові технології (дискусії, коментування, опонування тощо);
- рольове та імітаційне моделювання.

Інструменти, обладнання, програмне забезпечення

- навчальні посібники, вебінари;
- мультимедіа;
- персональні комп’ютери;
- 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	Для оцінювання рівня знань застосовується 100-бальна шкала оцінювання. Величина рівня

структура оцінки *COURSE GRADE COMPOSITION*	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 (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 (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
90-100	відмінно
82-89	Добре
74-81	Добре
64-73	задовільно
60-63	задовільно
0-59	незадовільно

Рекомендована література

Основна

1. Ромака В.А. Системи менеджменту інформаційної безпеки: Навчальний посібник / В.А. Ромака, В.Б. Дудикевич, Ю.Р. Гарасим, П.І. Гаранюк, І.О. Козлюк, Львів: Видавництво Львівської політехніки, 2012. 232 с.
2. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки: Навчальний посібник / О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник, Київ 2014. 189 с.
3. ДСТУ ISO 19011:2011 Настанови щодо здійснення аудитів систем управління, Київ Мінекономрозвитку України, 2013.
4. ДСТУ ISO/IEC 27000:2015 Методи захисту. Система менеджменту інформаційної безпеки. Огляд і словник. Київ ДП "УкрНДНЦ", 2016.
5. ДСТУ ISO/IEC 27000:2017 Інформаційні технології Методи захисту. Система менеджменту інформаційної безпеки. Огляд і словник термінів. Київ ДП "УкрНДНЦ" 2017.
6. ДСТУ ISO/IEC 27001:2015 Методи захисту систем управління інформаційною безпекою. Київ ДП "УкрНДЦ", 2016.
7. ДСТУ ISO/IEC 27002:2015 Звід практик щодо заходів інформаційної безпеки. Київ ДП "УкрНДНЦ", 2016.
8. ДСТУ ISO/IEC 27003:2018 Інформаційні технології Методи захисту. Системи керування інформаційною безпекою. Настанови. Київ ДП "УкрНДНЦ", 2018.

9. ДСТУ ISO/IEC 27004:2018 Інформаційні технології Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання. Київ ДП "УкрНДНЦ", 2018.
10. ДСТУ ISO/IEC 27005:2015 Інформаційні технології Методи захисту. Управління ризиками інформаційної безпеки. Київ ДП "УкрНДНЦ", 2016.
11. ДСТУ ISO/IEC 27006:2015 Інформаційні технології Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем керування інформаційною безпекою. Київ ДП "УкрНДНЦ", 2016.
12. ДСТУ ISO/IEC 27007:2015 Інформаційні технології Методи захисту. Настанова щодо аудиту керування інформаційною безпекою. Київ ДП "УкрНДНЦ", 2019. (англ.)
13. ISO/IEC 27007:2015 Інформаційні технології. методи безпеки. Настанови щодо управління інформаційною безпекою для телекомунікаційні організації на базі ISO / IEC 27002. (англ.)
14. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель. Київ ДП "УкрНДНЦ", 2017. (англ.)
15. ДСТУ ISO/IEC TR 1335-1:2003 Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки ІТ. Київ Держспоживстандарт України 2005.
16. ДСТУ ISO/IEC TR 1335-4:2005 Настанови з керування безпекою інформаційних технологій. Київ ДП "УкрНДНЦ", 2005.
17. Критерії безпеки комп'ютерних систем міністерства оборони США. (Помаранчева книга) 1985.

Допоміжна

1. Юдін О.К. Інформаційна безпека держави: Навчальний посібник/ О.К. Юдін, В.М. Богуш.- Харків: Консум, 2005.- 576 с.

Інформаційні ресурси в Інтернет

1. Стандарти серії ДСТУ/ISO 27000
http://online.budstandart.com/ua/catalog/doc-page.html?id_doc

2. Нормативні документи з технічного захисту інформації
https://cip.gov.ua/ua/news/perelik-dokumentiv-normativno-pravovoyi-bazi-sho-zabezpechuye-nadannya-vidpovidnikh-vidiv-poslug-u-galuzi-tekhnichnogo-zakhistu-informaciyi

Поєднання навчання та досліджень

Напрямок дослідження - проблеми впровадження менеджменту інформаційної безпеки 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=4526 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 №516 від [sDateTime_SignWriteAgree_Last]
Підписувач Сорока Валерій Степанович
Підписувач (дані КЕП): [oSignECP.sSigner_Sert]
Сертифікат 58E2D9E7F900307B04000000807E2D0054327D00