



Кафедра комп'ютерної інженерії та  
інформаційних технологій

## СИЛАБУС

<b>Базова інформація про дисципліну</b>	
<b>Назва дисципліни</b>	СЕ104 / Захист інформації в комп'ютерних системах та мережах / Protection of Information in Computer Systems and Networks
<b>Рівень вищої освіти</b>	Перший (бакалаврський)
<b>Галузь знань</b>	12 Інформаційні технології
<b>Спеціальність</b>	123 „Комп'ютерна інженерія”
<b>Освітня програма</b>	123 „Комп'ютерна інженерія ”
<b>Семестр</b>	1,2 семестри
<b>Курс</b>	1 курс (за скороченою формою навчання на базі ОКР молодший спеціаліст, ОС фаховий молодший бакалавр) 3 (повний термін навчання)
<b>Анотація курсу</b>	Навчальна дисципліна спрямована на формування уявлення про методи забезпечення надійності та захисту інформаційних ресурсів, комплекс вимог до системи забезпечення безпеки комп'ютерних систем, методи аналізу впливу загроз безпеки на комп'ютерні системи та мережі ефективний вибір та застосування засобів захисту, розробка стратегії та політик безпеки комп'ютерної системи.
<b>Сторінка курсу в MOODLE</b>	<a href="http://78.137.2.119:2929/course/view.php?id=15">http://78.137.2.119:2929/course/view.php?id=15</a>
<b>Мова викладання</b>	українська
<b>Лектор курсу</b>	Захарова Марія В'ячеславівна, к.т.н., доцент Канали комунікації: СДН «Moodle»: повідомлення в чаті E-mail: lecturer2020student@gmail.com
<b>Місце дисципліни в освітній програмі</b>	
<b>Освітня програма</b>	<a href="http://csbc.edu.ua/documents/otdel/ce.pdf">http://csbc.edu.ua/documents/otdel/ce.pdf</a>
<b>Перелік загальних компетентностей (ЗК)</b>	Здатність вчитися і оволодівати сучасними знаннями.

	<p>Знання та розуміння предметної області та розуміння професійної діяльності.</p> <p>Здатність застосовувати знання у практичних ситуаціях.</p> <p>Здатність працювати з інформацією, у тому числі у глобальних комп'ютерних мережах.</p>
<b>Перелік спеціальних компетентностей (СК)</b>	<p>Здатність забезпечувати захист інформації в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.</p> <p>Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.</p> <p>Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.</p>
<b>Перелік програмних результатів навчання</b>	<p>Вміти застосовувати знання для формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.</p> <p>Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації апаратних та програмних засобів комп'ютерної інженерії для вирішення технічних задач у професійній діяльності.</p>
<b>Опис дисципліни</b>	
<b>Структура навантаження на студента</b>	<p>Загальна кількість годин – 240</p> <p>Кількість кредитів – 8</p> <p>Кількість лекційних годин – 30</p> <p>Кількість практичних занять – 60</p> <p>Кількість годин для самостійної роботи студентів – 150</p> <p>Форма підсумкового контролю – залік, екзамен</p>
<b>Методи навчання</b>	<p>Словесні (інформаційна, самостійна робота з джерелами інформації, науково-популярна розповідь);</p> <p>Наочні (презентаційні повідомлення)</p> <p>Практичні (лабораторні роботи);</p> <p>Інтерактивні методи (дистанційні консультації).</p>
<b>Зміст дисципліни</b>	

<p><b>Тема 1.</b> Проблеми та напрямки забезпечення надійності в комп'ютерних системах (КС).</p>	<p>Напрямки забезпечення надійності КС.          Основні питання та визначення теорії надійності.          Політика безпеки, види політик безпеки.          Загрози безпеки інформації та канали проникнення в систему.          Основні вразливі місця комп'ютерних систем.</p>
<p><b>Тема 2.</b> Стратегії захисту інформації, характеристики стратегій</p>	<p>Оборонна, наступальна, випереджуюча стратегії захисту ресурсів КС.          Побудова систем захисту КС відповідно стратегій захисту.</p>
<p><b>Тема 3.</b> Методи і засоби захисту інформаційних ресурсів комп'ютерних систем.</p>	<p>Правові та організаційні методи захисту інформації комп'ютерних систем.          Криптографічний захист даних.          Програмні методи захисту інформації.          Фізичні методи і захисту інформації комп'ютерних систем.</p>
<p><b>Тема 4.</b> Суть та елементи теорії надійності.</p>	<p>Загальні положення теорії надійності.          Відмова і її види.          Комплексні показники надійності.          Показники довговічності та збережності.          Визначення показників надійності – інтенсивності, частоту та ймовірність відмов.</p>
<p><b>Тема 5.</b> Показники та фактори, що впливають на надійність КС та комп'ютерних мереж</p>	<p>Фактори, що впливають на функціональну надійність.          Конструктивні, виробничі та експлуатаційні фактори.          Об'єктивні та суб'єктивні фактори, що впливають на надійність обладнання систем.</p>
<p><b>Тема 6.</b> Підвищення надійності та захищеності КС.</p>	<p>Основні аспекти підвищення надійності, методи (структурне, функціональне, часове, інформаційне, навантажувальне резервування) та їх ознаки.          Визначення функції та коефіцієнт готовності відновлюваної системи за умови, що на неї діють прості потоки відмов і відновлень.          Підвищення надійності систем. Резервування</p>
<p><b>Тема 7.</b> Захист програмного забезпечення комп'ютерних систем</p>	<p>Категорії засобів захисту програмного забезпечення.          Програмні засоби захисту комп'ютерних систем.          Основні показники надійності ПЗ.          Моделі надійності ПЗ.</p>

<b>Тема 8.</b> Принципи забезпечення безпеки комп'ютерних мереж.	Надійність та відмова мережі. Методики визначення критеріїв надійності математичної моделі КМ.
<b>Тема 9.</b> Ідентифікація і аутентифікація користувачів	Поняття про ідентифікацію користувача та її особливості. Основні принципи та методи аутентифікації. Біометрична аутентифікація. Схеми аутентифікації та перевірки істинності.
<b>Тема 10.</b> Моделювання систем захисту інформаційних ресурсів.	Предмет, об'єкт захисту. Класифікація порушників безпеки. Принципи моделювання систем захисту інформації. Модель системи безпеки з повним перекриттям. Модель багаторівневого захисту інформації та інші.
<b>Тема 11.</b> Криптологічний захист інформаційних ресурсів.	Основні терміни та поняття. Криптографічні методи захисту інформації. Сучасні криптосистеми та їх особливості. Симетричні алгоритми шифрування інформації. Системи з відкритим ключем. Цифрові підписи. Адміністрування ключами.
<b>Тема 12.</b> Принципи побудови захищених систем. Стандарти із захисту інформації	Архітектура захищених операційних систем. Критерії безпеки комп'ютерних систем Методи і засоби захисту від атак через мережу Internet. Основні схеми мережного захисту на базі міжмережевих екранів Захист електронної пошти. Забезпечення безпеки електронних платежів. Світові стандарти із захисту даних в комп'ютерних системах. Державний стандарт України із захисту інформації.
<b>Політика дисципліни</b>	
<b>Політика відвідування</b>	Регулярне відвідування всіх видів занять, своєчасність виконання самостійної роботи. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання організується в он-лайн формі за погодженням із керівником курсу.
<b>Політика щодо дедлайнів та перескладання</b>	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.

<b>Академічна доброчесність</b>	У випадку недотримання політики академічної доброчесності (плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво) передбачено повторне проходження оцінювання.
---------------------------------	--

### Система оцінювання

Поточний контроль здійснюється протягом семестру під час проведення практичних, семінарських та інших видів занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що дозволяє студенту отримати атестацію з предмету – 60 балів); підсумковий/ семестровий контроль, проводиться у формі заліку (1 семестр) та іспиту (2 семестр), відповідно до графіку навчального процесу.

Підсумкова оцінка за умови заліку виставляється як загальна сума балів, набраних за результатами поточного контролю.

Підсумкова оцінка за умови іспиту виставляється як загальна сума балів набраних за результатами поточного (70%) та підсумкового контролю

#### Накопичування рейтингових балів з навчальної дисципліни (залік) 1 семестр

<b>Види навчальної роботи</b>	<b>Мах кількість балів</b>
Виконання практичних робіт № 1,2,3,5,6 по 5 балів	30
Виконання практичних робіт № 7,8 по 10 балів	20
Модульні контрольні роботи (2 к.р.)	20
Презентація	15
Індивідуальні практичні завдання	15
<b>Разом</b>	<b>100</b>

#### Накопичування рейтингових балів з навчальної дисципліни (екзамен) 2 семестр

<b>Види навчальної роботи</b>	<b>Мах кількість балів</b>
Виконання практичних робіт № 1,2,3,4 по 5 балів	20
Виконання практичних робіт № 5,6,7,8 по 5 балів	20
Індивідуальні завдання	30
Завдання екзамену	30
<b>Разом</b>	<b>100</b>

<b>Шкала оцінювання</b>		
<b>ECTS</b>	<b>Бали</b>	<b>Зміст</b>
<b>A</b>	90-100	Бездоганна підготовка в широкому контексті
<b>B</b>	80-89	Повні знання, міцні вміння
<b>C</b>	70-79	Хороші знання та вміння
<b>D</b>	65-69	Задовільні знання, стереотипні вміння
<b>E</b>	60-64	Виконання мінімальних вимог діяльності в стандартних умовах
<b>FX</b>	35-59	Слабкі знання, відсутність умінь
<b>F</b>	1-34	Необхідний повторний курс

### **Список рекомендованих джерел**

#### **Основна**

1. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.
2. Інформаційна безпека держави: навчальний посібник/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.
3. Cyber Security for Cyber Physical Systems / Saqib Ali, Taiseera Al Balushi, Zia Nadir, Omar Khadeer Hussain. – Cham, Switzerland : Springer, 2018. – 174 p.
4. Хорошко В. О. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.

#### **Додаткова**

1. Грищук Р.В. Основи кібернетичної безпеки: Монографія / Р.В. Грищук, Ю.Г. Даник; ред. Ю.Г. Данника. – Житомир: ЖНАЕУ, 2016. 636 с.
2. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2007. – 382 с.
3. Корченко А. О. Банківська безпека. / А. О. Корченко, Л. М. Скачек, В. О. Хорошко. – К. : ПВП «Задруга». – 2014. – 185 с.

4. Ластівка Г. І. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / Г. І. Ластівка, П. М. Шпатар – Чернівці: Чернівецький національний університет, 2018. - 252 с.
5. Методика та організація наукових досліджень: Навч. посіб. / С.Е. Важинський, Т.І. Щербак. – Суми: СумДПУ імені А. С. Макаренка, 2016. – 260 с.
6. Надійність, контроль комп'ютерних систем та мереж [Текст]: конспект лекцій для студентів спеціальності 123 – «Комп'ютерна інженерія» денної та заочної форм навчання / уклад. О.І. Міскевич, К.Я.Бортник. – Луцьк: Луцький НТУ, 2017. – 44 с.
7. Нормування показників надійності технічних засобів : навчальний посібник / О. М. Васілевський, О. Г. Ігнатенко. – Вінниця : ВНТУ, 2013. – 160 с.
8. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / Рибальський О.В., Смаглюк В.М., Хахановський В.Г. – К.: НАВС, 2013. – 255 с.
9. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
10. Федун І. В. Основи теорії надійності та контролю якості виробів електронної техніки: Лабораторний практикум. – Вінниця: ВДТУ, 2003. – 71 с.
11. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations / Edited by Fei Hu. – Taylor & Francis Group, 2016. – 564 p.