

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Методи та засоби захисту біомедичної інформації»

№	Назва	Опис
1	Назва факультету	Електронної та біомедичної інженерії (ЕЛБІ)
2	Рівень вищої освіти	Другий (магістерський)
3	Код і назва спеціальності	163 – Біомедична інженерія (БМІ)
4	Тип і назва освітньої програми	Освітньо-професійна програма «Біомедична інженерія»
5	Назва дисципліни	МЗЗБМІ
6	Кількість ЄКТС кредитів	5
7	Структура дисципліни (розподіл за видами та годинами навчання)	лекції – 26 годин; практичні заняття – 4 години; лабораторні заняття – 20 годин; консультації – 10 годин; самостійна робота – 90 годин; семестровий контроль – залік .
8	Графік вивчення дисципліни	1 курс магістерського рівня вищої освіти, 2 семестр
9	Передумови для навчання дисципліною за	Базується на знаннях, отриманих з таких навчальних дисциплін: «Спеціальні розділи вищої математики», «Медична інформатика», «Біоінформатика», «Методи обробки біомедичних даних». ПРН2. Аналізувати і вирішувати складні медико-інженерні та біоінженерні проблеми із застосуванням математичних методів та інформаційних технологій. ПРН4. Розробляти, планувати, виконувати та обґрунтовувати інноваційні проекти біоінженерних об'єктів та систем медико-технічного призначення з урахуванням інженерних, медичних, правових, економічних, екологічних та соціальних аспектів, здійснювати їх інформаційне та методичне забезпечення.
10	Анотація дисципліни	Основні змістові модулі лекцій Змістовий модуль 1. Основні поняття інформаційної безпеки медичних даних. Класичні симетричні криптосистеми захисту біомедичної інформації. Змістовий модуль 2. Класичні асиметричні криптосистеми та методи автентифікації, біометричної ідентифікації. Змістовий модуль 3. Загальні відомості відносно

		методів криптоаналізу двоключових криптосистем. Алгоритми факторизації біомедичної інформації. Теми лабораторних занять 1. Дослідження алгоритмів та програмних засобів симетричного шифрування біомедичних даних. 2. Дослідження афінного перетворення алгоритму RJNDAEL для захисту біомедичної інформації. 3. Аналіз та дослідження алгоритму несиметричного цифрового підпису RSA. 4. Аналіз та дослідження алгоритму несиметричного цифрового підпису Ель-Гамала. 5. Вивчення способу біометричної аутентифікації в АСОД.
	Компетентності, знання, вміння, розуміння, якими оволодіє здобувач вищої освіти в сфері навчання	Зн2 Критичне осмислення основних теорій, принципів, методів і понять у навчанні та професійній діяльності Зн1 Концептуальні знання, набуті у процесі навчання та професійної діяльності, включаючи певні знання сучасних досягнень. Ум1 Розв’язання складних непередбачуваних задач і проблем у спеціалізованих сферах професійної діяльності та/або навчання, що передбачає збирання та інтерпретацію інформації (даних), вибір методів та інструментальних засобів, застосування інноваційних підходів. АВ3 Здатність до подальшого навчання з високим рівнем автономності. АВ1 Управління комплексними діями або проектами, відповідальність за прийняття рішень у непередбачуваних умовах.
12	Результати навчання здобувача вищої освіти	За результатом вивчення дисципліни студенти повинні: ЗНАТИ: - основні положення політики інформаційної безпеки у біомедичній інженерії; - визначення, класифікацію та основні властивості криптографічних систем та протоколів; - математичні моделі криптографічних перетворень; - криптографічні алгоритми, які реалізують перетворення біомедичної інформації; - новітні технології захисту даних в галузі біомедичної інженерії. ВМІТИ:

		- на практиці втілювати політику інформаційної безпеки, використовувати організаційні, технічні, алгоритмічні та інші методи і засоби захисту біомедичної інформації; - практично реалізовувати обчислювальні алгоритми криптографічного перетворення, зокрема, алгоритми шифрування, ґешування, цифрового підпису тощо; - оцінювати стійкість криптографічних систем до різних атак.
13	Система оцінювання відповідно до кожного завдання для складання заліку/іспиту	Якісні критерії оцінювання <i>Задовільно, D, E (60-74).</i> Виставляється, якщо студент відпрацював та захистив всі лабораторні роботи, виконав індивідуальні завдання, засвоїв основні поняттями навчального матеріалу, може самостійно відтворити значну частину навчального матеріалу і робити певні узагальнення, ознайомився з основною літературою, рекомендованою програмою, вміє виконувати навчальні завдання, передбачені програмою. <i>Добре, C (75-89).</i> Виставляється, якщо студент відпрацював та захистив всі лабораторні роботи, виконав індивідуальні завдання, вільно володіє навчальним матеріалом, вміє застосовувати вивчений матеріал у стандартних ситуаціях, узагальнювати та систематизувати навчальну інформацію, самостійно виконує передбачені програмою навчальні знання, самостійно знаходить і виправляє допущені помилки, може аргументовано обрати раціональний спосіб виконання навчального завдання. <i>Відмінно, A, B (90-100).</i> Виставляється, якщо студент відпрацював та захистив всі лабораторні роботи, виконав індивідуальні завдання, його знання, вміння і навички повністю відповідають вимогам програми, володіє глибокими, міцними знаннями, самостійно визначає проміжні цілі і вміє планувати особисту навчальну діяльність, оцінювати результати власної практичної роботи, вміє знаходити додаткову інформацію та самостійно використовує її для реалізації поставлених перед ним навчальних цілей, судження його логічні і достатньо обґрунтовані, засвоїв взаємозв'язок основних понять дисципліни, їх значення для подальшої професійної діяльності, вміє вільно використовувати сучасні програмні засоби для поповнення власних знань

		та розв'язування задач. Якісні критерії оцінювання знань та вмінь студента на заліку. <i>Задовільно, D, E (60-74).</i> Показати необхідний мінімум теоретичних знань. Обрати метод розв'язання задачі. <i>Добре, C (75-89).</i> Твердо знати головні теми теоретичного матеріалу. Розв'язати задачу. <i>Відмінно, A, B (90-100).</i> Показати повні знання теоретичного матеріалу. Безпомилково розв'язати задачу, пояснити та обґрунтувати обраний метод розв'язання. Кількісні критерії оцінювання: <table> <tr> <th>Вид заняття / контрольний захід</th> <th>Оцінка $O_{\text{сем}}$</th> </tr> <tr><td>ЛБ № 1</td><td>10</td></tr> <tr><td>ЛБ № 2</td><td>10</td></tr> <tr><td>Контрольна робота № 1</td><td>20</td></tr> <tr><td>Практичне заняття</td><td>5</td></tr> <tr><td>Контрольна точка 1</td><td>50</td></tr> <tr><td>ЛБ № 3</td><td>10</td></tr> <tr><td>ЛБ № 4</td><td>10</td></tr> <tr><td>ЛБ № 5</td><td>10</td></tr> <tr><td>Практичне заняття 2</td><td>5</td></tr> <tr><td>Контрольна робота №2</td><td>20</td></tr> <tr><td>Контрольна точка 2</td><td>50</td></tr> <tr><td>Всього за семестр</td><td>60....100</td></tr> </table>	Вид заняття / контрольний захід	Оцінка $O_{\text{сем}}$	ЛБ № 1	10	ЛБ № 2	10	Контрольна робота № 1	20	Практичне заняття	5	Контрольна точка 1	50	ЛБ № 3	10	ЛБ № 4	10	ЛБ № 5	10	Практичне заняття 2	5	Контрольна робота №2	20	Контрольна точка 2	50	Всього за семестр	60....100
Вид заняття / контрольний захід	Оцінка $O_{\text{сем}}$																											
ЛБ № 1	10																											
ЛБ № 2	10																											
Контрольна робота № 1	20																											
Практичне заняття	5																											
Контрольна точка 1	50																											
ЛБ № 3	10																											
ЛБ № 4	10																											
ЛБ № 5	10																											
Практичне заняття 2	5																											
Контрольна робота №2	20																											
Контрольна точка 2	50																											
Всього за семестр	60....100																											
14	Якість освітнього процесу	Основні методи навчання – практичний (лабораторні); наочний (метод ілюстрацій і метод демонстрацій); словесний (лекція); робота з навчально-методичною літературою (конспектування); відеометод у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (мультимедійні). Засоби оцінювання – залік; контрольна робота; виконання лабораторних робіт та оформлення звітів. Студенти повинні своєчасно відпрацювати та захистити лабораторні роботи, виконання практичних завдань, тезисне конспектування основних розділів лекційних занять, під час контрольних робіт дотримуватися правил академічної доброчесності.																										
15	Методичне забезпечення	1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний підручник. Харків, ХНУРЕ, 2011 р. 2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2011 р.																										

		3. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с. 4. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с.
16	Розробник силабусу	Доцент кафедри БІТ ХНУРЕ, Сєверінов Олександр Васильович, oleksandr.sievierinov@nure.ua