

44-2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
ІМ. М. С. ЖУКОВСЬКОГО
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Кафедра Радіоелектронних та біомедичних комп'ютеризованих
засобів і технологій (№ 502)

«ЗАТВЕРДЖУЮ»

Керівник проектної групи


(підпис)

О. Й. Довнар
(ініціали та прізвище)

«31» серпня 2023 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕХНОЛОГІЇ ЗАХИСТУ МЕДИЧНОЇ ІНФОРМАЦІЇ

(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: 122 «Комп'ютерні науки»
(код і найменування спеціальності)

Освітня програма: «Комп'ютерні технології в біології та медицині»
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2023 рік

Робоча програма Технології захисту медичної інформації _____
(назва дисципліни)

для студентів за спеціальністю 122 «Комп'ютерні науки»
освітньою програмою «Комп'ютерні технології в біології та медицині»

« 31 » серпня 2023 р., – 12 с.

Розробники:

ЛОМОНОСОВ Юрій, доцент кафедри радіоелектронних і біомедичних
комп'ютеризованих засобів і технологій (№ 502), к.т.н., доцент _____
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри радіоелектронних і біо-
медичних комп'ютеризованих засобів і технологій (№ 502)

(назва кафедри)

Протокол № 1 від 31» серпня 2023 р.

Завідувач кафедри д.т.н., професор _____
(науковий ступінь та вчене звання) (підпис) Олена ВИСОЦЬКА
(ініціали та прізвище)

1. Опис навчальної дисципліни

Найменування показника	Галузь знань, спеціальність, освітня програма, рівень вищої освіти	Характеристика навчальної дисципліни (денна форма навчання)
Кількість кредитів – 5,5	Галузь знань <u>12 «Інформаційні технології»</u> <small>(шифр і найменування)</small> Спеціальність <u>122 «Комп'ютерні науки»</u> <small>(код і найменування)</small> Освітня програма <u>«Комп'ютерні технології в біології та медицині»</u> <small>(найменування)</small> Рівень вищої освіти: <u>перший (бакалаврський)</u>	Цикл професійної підготовки Обов'язкова
Кількість модулів – 1		Навчальний рік
Кількість змістовних модулів – 2		2023/2024
Індивідуальне завдання – <u>не передбачене</u> <small>(назва)</small>		Семестр
Загальна кількість годин – 60/ 165		8-й
Кількість тижневих годин для денної форми навчання: аудиторних – 3,5 самостійної роботи здобувача – 5,9		Лекції*
		<u>36</u>
		Практичні, семінарські*
		<u>24</u>
		Лабораторні*
	Самостійна робота	
	<u>105</u>	
	Вид контролю	
	модульний контроль, залік	

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

60 годин аудиторних занять / 165 годин самостійної роботи.

*Аудиторне навантаження може бути зменшене або збільшене на одну годину залежно від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: надати студентам знань з методів та засобів забезпечення інформаційної безпеки, захисту інформаційних ресурсів та об'єктів критичної інфраструктури.

Завдання: вивчити основні методології захисту інформації для створення надійних медичних інформаційних систем.

Компетентності, які набуваються:

- здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів комп'ютерних наук в області біології та медицини і характеризується комплексністю та невизначеністю умов (ІК);
- здатність до абстрактного мислення, аналізу та синтезу (ЗК1);
- здатність застосовувати знання у практичних ситуаціях (ЗК2);
- знання та розуміння предметної області та розуміння професійної діяльності (ЗК3);
- здатність проектувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: узагальненого, об'єктно-орієнтованого, функціонального, логічного, з відповідними моделями, методами й алгоритмами обчислень, структурами даних і механізмами управління (СК8);
- здатність реалізувати багаторівневу обчислювальну модель на основі архітектури клієнт-сервер, включаючи бази даних, знань і сховища даних, виконувати розподілену обробку великих наборів даних на кластерах стандартних серверів для забезпечення обчислювальних потреб користувачів, у тому числі на хмарних сервісах (СК9);
- здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення (СК12);
- здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури (СК14).

Очікувані результати навчання:

– володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного (ПР13);

– володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення (ПР 14);

– розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних (ПР16);

– застосовувати сучасні підходи для розв'язання нових проблем, що виникають в сфері комп'ютерних технологій біології та медицини, враховуючи соціальні, біоетичні, біофізичні та економічні аспекти, існуючі державні і закордонні стандарти; забезпечувати ефективне управління якістю інформаційного, алгоритмічного та програмного забезпечення медичних комп'ютерних систем на основі використання сучасних моделей, методів та інструментальних засобів (ПР19).

Пререквізити – „Вища математика”, „Алгоритмізація та програмування”, „Медичні інформаційні системи”.

Кореквізити – „Методи та засоби захисту медичної інформації в інформаційно-комунікаційних системах”.

3. Зміст навчальної дисципліни

Модуль 1.

Змістовий модуль 1. Основи захисту медичної інформації

Тема 1. Вступ до дисципліни «Технології захисту медичної інформації»

Загальне уявлення про інформаційну безпеку. Види загроз для комп'ютерної медичної інформації. Засоби протидії загрозам для комп'ютерної інформації. Поняття про комп'ютерні злочини. Визначення, аналіз та фіксація слідів комп'ютерних злочинів

Тема 2. Загальний захист медичних електронних документів при зберіганні та передачі в інформаційно-комунікаційних системах.

Основні положення крипто аналізу та крипто захисту. Захист електронних документів за допомогою симетричних методів шифрування. Захист електронних документів за допомогою встановлення ключів доступу. Методи декодування ключів доступу до електронних документів. Надійність захисту електронних документів при симетричному шифруванні та за допомогою кодів доступу.

Тема 3. Технічне та юридичне забезпечення електронного цифрового підпису як засобу несиметричного шифрування.

Електронний бізнес та електронна комерція. Закони України “Про електронний документ та електронний документообіг” та «Про електронний цифровий підпис». Поняття про електронний цифровий підпис. Несиметричні методи шифрування. Поняття про дайджест повідомлення. Поняття про криптостійкість засобів ЕЦП. Програмне, технічне та юридичне забезпечення ЕЦП.

Тема 4. Інформаційні технології захисту авторських прав на мультимедійні твори.

Юридичні та технічні проблеми захисту медичної інформації у цифровому вигляді. Основні визначення та принципи стеганографії. Огляд стеганографічних методів. Цифрові водяні знаки. Захист електронних документів за допомогою ЦВЗ. Захист цифрових зображень за допомогою ЦВЗ. Захист аудіоданих за допомогою ЦВЗ. Захист відеоданих за допомогою ЦВЗ.

Модульний контроль.

Змістовий модуль 2. Комп’ютерна вірусологія та ідентифікація користувачів в інформаційно-комунікаційних системах.

Тема 1. Лінгвістична безпека медичних електронних документів.

Види та методи автороведчеської експертизи. Формальні та статистичні методи автороведчеської експертизи. Комп’ютерні програми визначення авторства тексту.

Тема 2. Ідентифікація користувачів як засіб захисту інформаційно-комунікаційних систем.

Управління доступом до інформаційних ресурсів комп’ютерних систем. Сучасні підходи до задачі ідентифікації користувачів інформаційних систем. Системи захисту за допомогою ключів доступу. Апаратна та електронна ідентифікація користувачів. Біометрична ідентифікація користувачів. Комплексна (багатофакторна) ідентифікація користувачів

Тема 3. Комп'ютерна вірусологія та антивірусний захист даних.

Основи комп'ютерної вірусології. Класифікація комп'ютерних вірусів. Антивірусні засоби та принципи захисту даних. Архівація даних як засіб захисту від комп'ютерних вірусів.

Тема 4. Виявлення та дослідження віртуальних (електронних) слідів користувача в інформаційно-комунікаційних системах.

Значення та зміст лог - файлів. Види лог – файлів. Виявлення та попереднє дослідження лог - файлів Журнал подій веб - браузера (Посилання, завантаження, закладки). Структура баз даних IP реєстраторів у мережі Internet (IP Registry). Перетворення повідомлення E-mail у текстовий файл за допомогою функцій поштових сервісів. Визначення часу отримання повідомлення по E-mail та IP адресу відправника. Виявлення та встановлення приналежності IP адреси відправника повідомлення. Виявлення та попереднє дослідження розташування сервера Internet реєстратора за вказаною IP адресою. Виявити та визначити діапазон IP адресів у блоці, до якого належить IP адреса відправника повідомлення. Виконати трасування IP адреси відправника повідомлення. Виявити та визначити IP адресу передостаннього хоста у списку IP адрес. При on-line режимі роботи знайти та визначити MAC адресу відправника повідомлень. За допомогою MAC адресу встановити виробника і тип мережевого адаптера відправника повідомлень.

Модульний контроль.

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с.р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1. Основи захисту медичної інформації					
Тема 1. Вступ до дисципліни «Технології захисту медичної інформації»	15	4	2	–	9
Тема 2. Загальний захист медичних електронних документів при зберіганні та передачі в інформаційно-комунікаційних системах.	18	4	4	–	10
Тема 3. Технічне та юридичне забезпечення електронного цифрового підпису як засобу несиметричного шифрування.	22	4	2	–	16
Тема 4. Інформаційні технології захисту авторських прав на мультимедійні твори.	22	6	2	–	14

Модульний контроль	2	–	2	–	–
Разом за змістовим модулем 1	79	18	12	0	49
Змістовий модуль 2. Комп'ютерна вірусологія та ідентифікація користувачів в інформаційно-комунікаційних системах.					
Тема 1. Лінгвістична безпека медичних електронних документів.	20	4	2		14
Тема 2. Ідентифікація користувачів як засіб захисту інформаційно-комунікаційних систем.	20	4	2		14
Тема 3. Комп'ютерна вірусологія та антивірусний захист даних.	22	4	4		14
Тема 4. Виявлення та дослідження віртуальних (електронних) слідів користувача в інформаційно-комунікаційних системах.	22	6	2		14
Модульний контроль	2	–	2		–
Разом за змістовим модулем 2	86	18	12	0	56
Усього годин	165	36	24	0	105

5. Теми семінарських занять

№ п/п	Назва теми	Кількість годин
1	Не передбачено навчальним планом	–
	Разом	–

6. Теми практичних занять

№ п/п	Назва теми	Кількість годин
1	Вступ до дисципліни «Технології захисту медичної інформації»	2
2	Загальний захист медичних електронних документів при зберіганні та передачі в інформаційно-комунікаційних системах.	4
3	Технічне та юридичне забезпечення електронного цифрового підпису як засобу несиметричного шифрування.	2
4	Інформаційні технології захисту авторських прав на мультимедійні твори.	2
5	Модульний контроль № 1	2
6	Лінгвістична безпека медичних електронних документів.	2
7	Ідентифікація користувачів як засіб захисту інформаційно-комунікаційних систем.	2

№ п/п	Назва теми	Кількість годин
8	Комп'ютерна вірусологія та антивірусний захист даних.	4
9	Виявлення та дослідження віртуальних (електронних) слідів користувача в інформаційно-комунікаційних системах.	2
10	Модульний контроль № 2	2
	Разом	24

7. Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Не передбачено навчальним планом	–
	Разом	–

8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Вступ до дисципліни «Технології захисту медичної інформації»	9
2	Загальний захист медичних електронних документів при зберіганні та передачі в інформаційно-комунікаційних системах.	10
3	Технічне та юридичне забезпечення електронного цифрового підпису як засобу несиметричного шифрування.	16
4	Інформаційні технології захисту авторських прав на мультимедійні твори.	14
5	Лінгвістична безпека медичних електронних документів.	14
6	Ідентифікація користувачів як засіб захисту інформаційно-комунікаційних систем.	14
7	Комп'ютерна вірусологія та антивірусний захист даних.	14
8	Виявлення та дослідження віртуальних (електронних) слідів користувача в інформаційно-комунікаційних системах.	14
	Разом	105

9. Індивідуальні завдання

Не передбачені навчальним планом.

10. Методи навчання

Застосовуються наступні методи навчання: словесні, наочні та практичні, а саме: проведення аудиторних лекцій (із застосуванням пояснювально-

ілюстративного та проблемного викладання навчального матеріалу), виконання практичних завдань та лабораторних робіт, консультації протягом семестру, самостійна робота студентів за матеріалами, опублікованими кафедрою (методичні посібники).

11. Методи контролю

Поточний контроль – виконання практичних завдань та лабораторних робіт, оформлення звітів та здача матеріалу тем лабораторних робіт.

Тестовий контроль – проведення модульних контрольних робіт.

Семестровий контроль – залік.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1			
Змістовний модуль 1			
Робота на лекціях	0...1	9	0...9
Робота на практичних заняттях	0...5	6	0...30
Модульний контроль	0...11	1	0...11
Змістовний модуль 2			
Робота на лекціях	0...1	9	0...9
Робота на практичних заняттях	0...5	6	0...30
Модульний контроль	0...11	1	0...11
Усього за семестр			0...100

Залік проводиться у вигляді комп'ютерного тесту. Студенту надається 15 запитань різного рівня складності (теоретичних питань та практичних завдань) з 5 варіантами відповідей. Тільки один варіант відповіді є вірним. За кожну вірну відповідь студент отримує від 5 до 8 балів (залежно від рівня складності завдання) На здачу комп'ютерного тесту відводиться фіксований час – 90 хвилин.

Всього (за умов надання всіх вірних відповідей) студент отримує:

$$5 \text{ завдань} \times 5 \text{ балів} + 5 \text{ завдань} \times 7 \text{ балів} + 5 \text{ завдань} \times 8 \text{ балів} = 100 \text{ балів.}$$

Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60-74). Показати мінімально-достатній рівень знань та умінь. Вміти викладати отримані знання в усній чи письмовій формі; при цьому, неповний обсяг засвоєного навчального матеріалу не повинен перешкоджати засвоєнню наступного програмного матеріалу; допускаються окремі істотні

помилки, виправлені за допомогою викладача. Виконати всі практичні завдання. Виконати та захистити всі лабораторні роботи з навчальної дисципліни. Відповідати на теоретичні питання на елементарному рівні в межах конспекту лекцій. Вирішувати найпростіші задачі модульного контролю. Вміти пояснити типові алгоритми та програмні рішення, що використовувалися під час виконання лабораторних робіт.

Добре (75-89). Показати середній рівень знань та умінь. Викладати отримані знання в усній чи письмовій формі у достатньому обсягу, системно, відповідно до вимог навчальної програми (допускаються окремі несуттєві помилки, що виправляються студентом після указівки викладача). Виділяти істотні ознаки вивченого за допомогою операцій аналізу і синтезу; підкріпляти вивчений матеріал відомими фактами і відомостями; виявляти причинно-наслідкові зв'язки досліджуваних процесів та явищ; формулювати висновки і узагальнення, у яких можуть бути окремі несуттєві помилки. Виконати всі практичні завдання. Виконати та захистити всі лабораторні роботи з навчальної дисципліни. Відповідати на теоретичні питання на достатньому рівні в межах конспекту лекцій та рекомендованих підручників, вміти обґрунтовано обирати типові рішення. Вирішувати задачі модульного контролю середнього рівня складності. Вміти розробляти типові алгоритми та програмні рішення, подібні використовуваним на лабораторних заняттях.

Відмінно (90-100). Показати відмінний рівень знань та умінь. Викладати отримані знання в усній чи письмовій формі у повному обсягу, системно, відповідно до вимог навчальної програми (припустимими є одиничні несуттєві помилки, які студент виправляє самостійно). Виділяти істотні ознаки вивченого за допомогою операцій аналізу і синтезу; вільно оперувати відомими фактами і відомостями; виявляти причинно-наслідкові зв'язки досліджуваних процесів та явищ; формулювати висновки і узагальнення. Виконати всі практичні завдання. Виконати та захистити всі лабораторні роботи з навчальної дисципліни. Відповідати на теоретичні питання на високому рівні в межах конспекту лекцій, рекомендованих підручників та додаткової літератури, вміти аналізувати надану інформацію та пропонувати нестандартні рішення, вміти їх обґрунтовувати. Вирішувати задачі модульного контролю високого рівня складності. Вміти розробляти алгоритми та програмні рішення, відмінні від використовуваних на лабораторних заняттях.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

Пашнєв Д.В., Рудик М.В. Принципи захисту комп'ютерної інформації від неправомірного втручання [Електронний ресурс]. – Режим доступу: URL: http://www.nbu.gov.ua/portal/soc_gum/nvdduvs/2010_2/Pashnev_Rudik.pdf – Назва з екрану.

Голубів В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навч. посібник / За заг. ред. доктора юридичних наук, професора Р. А. Калюжного. - Запоріжжя: ГУ "ЗІДМУ", 2002. - 292 с. – С. 15-30, С. 100-110.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Щербаковський М. Г. Розслідування комп'ютерних злочинів : посібник / М. Г. Щербаковський, Д. В. Пашнєв ; МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2010. – 112 с. – С. 25-39.

Греков, І.П. Принципи захисту комп'ютерної інформації від неправомірного втручання [Текст] / І.П. Греков, Ю.С. Логвин // Сучасні інформаційні системи і технології : матеріали Першої міжнародної науково-практичної конференції, м. Суми, 15-18 травня 2012 р. / Ред.кол.: А.С. Довбиш, О.А. Борисенко, І.В. Баранова. — Суми : СумДУ, 2012. — С. 219-221.

Голубів В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навч. посібник / За заг. ред. доктора юридичних наук, професора Р. А. Калюжного. - Запоріжжя: ГУ "ЗІДМУ", 2002. - 292 с. – С. 31-42.