

Міністерство охорони здоров'я України
Полтавський державний медичний університет

Кафедра фізики

«УЗГОДЖЕНО»

Гарантом освітньо-професійної програми
«Біологія»

«28» серпня 2024 року

«ЗАТВЕРДЖЕНО»

Головою вченої ради міжнародного
факультету

Протокол від 28 серпня 2024 р. № 1

СИЛАБУС

Цифрові технології в ОЗ. Кібербезпека та кібергігієна

обов'язкова

рівень вищої освіти
галузь знань
спеціальність
кваліфікація освітня
освітньо-професійна програма
форма навчання
курс(и) та семестр(и) вивчення навчальної
дисципліни

першого (бакалаврського) рівня вищої освіти
09 Біологія
091 Біологія
Бакалавр з біології
Біологія
Заочна (дистанційна)
I курс I семестр

«УХВАЛЕНО»

на засіданні кафедри фізики

Протокол від 28 серпня 2024 р. № 1

ДАНІ ПРО ВИКЛАДАЧІВ, ЯКІ ВИКЛАДАЮТЬ НАВЧАЛЬНУ ДИСЦИПЛІНУ

Прізвище, ім'я, по батькові викладача (викладачів), науковий ступінь, учене звання	Сілкова Олена Вікторівна – к. пед. н, доцент Коровіна Лідія Дмитрівна- к. б.н., ст.викладач
Профайл викладача (викладачів)	https://www.pdmu.edu.ua/fakultets/foreign-students/kafedry/med-inform/workers
Контактний телефон	(0532) 68-73-86
E-mail:	med_informatic@pdmu.edu.ua
Сторінка кафедри на сайті ПДМУ	https://www.pdmu.edu.ua/fakultets/foreign-students/kafedry/med-inform

ОСНОВНІ ХАРАКТЕРИСТИКИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Обсяг навчальної дисципліни

Кількість кредитів / годин – **5,0 / 150**, із них:

Лекції (год.) – **6**

Практичні (год.) – **14**

консультацій - **10**

Самостійна робота (год). – **120**

Вид контролю – **Підсумковий модульний контроль**

Політика навчальної дисципліни

Для успішного проходження курсу та складання підсумкового модульного контролю необхідним є відвідування лекцій, вчасне вивчення навчального матеріалу у повному обсязі згідно з планом практичних занять та виконання самостійної роботи.

Для успішного засвоєння навчального матеріалу здобувач вищої освіти зобов'язаний:

- приходити на заняття вчасно;
- відвідати усі практичні заняття (у разі відсутності – відпрацювати);
- самостійно освоїти матеріал пропущеного заняття;
- сумлінно готуватися до заняття;
- активно працювати на занятті;
- відключати телефон на занятті (якщо немає потреби у його використанні);
- бути чемним, толерантним та ввічливим, відкритим до конструктивної дискусії;
- не допускати порушення академічної доброчесності під час проектної, індивідуальної та самостійної діяльності.

При організації освітнього процесу в ПДМУ викладачі і здобувачі вищої освіти діють відповідно до «Положення про організацію освітнього процесу в Полтавському державному медичному університеті», «Положення про

академічну добротність» та інших діючих нормативних документів, розташованих на сайті університету: <https://www.pdmu.edu.ua/n-process/department-npr/normativni-dokumenti> Проведення освітнього процесу за дисципліною «Цифрові технології в ОЗ. Кібербезпека та кібергігієна» відбувається з використанням технологій дистанційного навчання, зокрема лекції та практичні заняття проводяться з використанням платформи ZOOM, Google Meet, Google Classroom та ін.

Опис навчальної дисципліни

Цифрові технології в ОЗ. Кібербезпека та кібергігієна - це інтегральна міждисциплінарна наука, що виникла на перетині інформатики, комп'ютерних технологій та біології. Ця дисципліна стосується ресурсів, баз даних, алгоритмів та методів, які необхідні для оптимізації отримання, зберігання, передачі та використання інформації в галузі охорони здоров'я та біомедицини, ознайомлення з основами та фундаментальними поняттями в галузі кібербезпеки, кібергігієни. Сфера застосувань дисципліни є багатопрофільною та охоплює такі галузі, як електронні медичні картки пацієнтів, системи підтримки прийняття рішень. eHealth, телемедицина, медична етика, використання комп'ютерних технологій у біологічних дослідженнях, надає загальне уявлення про сутність кібербезпеки, кібергігієни та їх важливість в сучасному цифровому світі.

Здобувачі вищої освіти отримують професійні навички пошуку та аналізу інформації біомедичного профілю, використання інноваційних програм, ресурсів та комп'ютерних технологій для покращення охорони здоров'я, для розвитку науково-обґрунтованої медицини та управління у галузі біології, медицини, проведення власних досліджень, дізнаються про різноманітні види кіберзагроз, включаючи хакерські атаки, віруси, фішинг, витік даних тощо, та навчаються оцінювати ризики для організацій та індивідів, основним принципам та методам захисту інформації, включаючи шифрування, аутентифікацію, авторизацію та інші механізми.

Отримані ними компетенції будуть потрібні для роботи в лікарнях, науково-дослідних лабораторіях, діагностичних лабораторіях, страхових компаніях та урядових організаціях.

Цей курс надає необхідну базу для подальшого вивчення та розвитку інформаційних технологій у біології, призначений для тих, хто прагне зрозуміти основи захисту від кіберзагроз та небезпек, що існують у цифровому світі, зокрема медичному.

Пререквізити і постреквізити навчальної дисципліни:

- базується на вивченні здобувачами вищої освіти навчальних дисциплін: медична та біологічна фізика, медична біологія, морфологічних дисциплін й інтегрується з цими дисциплінами;
- закладає основи вивчення дисципліни соціальна медицина, громадське здоров'я; сприяє вивченню здобувачами вищої освіти клінічних, гігієнічних та соціальних дисциплін; передбачає формування умінь застосовувати знання з

кібербезпеки, кібергігієни, медичної інформатики в процесі подальшого навчання у професійній діяльності.

Мета та завдання навчальної дисципліни:

– метою вивчення навчальної дисципліни є: формування та розвиток компетенцій, спрямованих на застосування сучасних комп'ютерних технологій у біології, медицині та охороні здоров'я, отримання знань про методи інформатизації подальшої діяльності, автоматизації клінічних досліджень, комп'ютеризації управління у системі охорони здоров'я; вміння використовувати сучасне програмне забезпечення загального та спеціального призначення при опрацюванні медико-біологічних даних. формування цілісного уявлення про кібербезпеку, кібергігієну та базових знань в даній галузі.;

– основними завданнями вивчення дисципліни є:

1) формування та розвиток знань, умінь і навичок, необхідних для ефективного використання сучасних програм загального та спеціального призначення у галузі охорони здоров'я;

2) ознайомлення здобувачів вищої освіти із значенням та можливостями нових інформаційно-комунікаційних технологій у галузі охорони здоров'я, з перспективами розвитку комп'ютерних технологій; різноманітними видами кіберзагроз, включаючи хакерські атаки, віруси, фішинг, витік даних;

3) розвиток уміння самостійно опановувати програмні засоби різного призначення та оновлювати й інтегрувати набуті знання, оцінювати ризики кібербезпеки для організацій та індивідів;

4) пояснення принципів формалізації і алгоритмізації медичних задач, принципи моделювання в біології та медицині;

5) формування базових навичок щодо роботи з персональним комп'ютером (ПК), пошуку медичної інформації з використанням інформаційних технологій, основних принципів захисту інформації, включаючи шифрування, аутентифікацію, авторизацію та інші механізми.;

6) використання методів опрацювання медико-біологічних даних, захисту інформації.

Цілі сталого розвитку:

1. ЦСР 3: Міцне здоров'я і благополуччя. Основна мета дисципліни — сприяти розвитку медичних технологій, діагностики, лікування.
2. ЦСР 4: Якісна освіта. Використання інформаційних технологій для навчання медичних фахівців.
3. ЦСР 9: Індустріалізація, інновації та інфраструктура. Розробка новітніх медичних пристроїв і технологій.
4. ЦСР 10: Зменшення нерівності. Надання доступу до якісних медичних технологій в регіонах або для вразливих груп.
5. ЦСР 12: Відповідальне споживання і виробництво. Створення енергоефективних та екологічних медичних пристроїв.
6. ЦСР 17: Партнерство заради сталого розвитку. Співпраця між науковими установами, медичними закладами, ІТ-компаніями.

Компетентності та результати навчання згідно з освітньо-професійною програмою, формуванню яких сприяє дисципліна

Дисципліна «Цифрові технології в ОЗ. Кібербезпека та кібергігієна» забезпечує набуття здобувачами вищої освіти **компетентностей**:

інтегральна: здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі біології при здійсненні професійної діяльності або у процесі навчання, що передбачає застосування законів, теорій та методів біологічної науки і характеризується комплексністю та невизначеністю умов.

Загальні:

ЗК03. Здатність генерувати нові ідеї (креативність).

ЗК 7. Здатність вчитися і оволодівати сучасними знаннями.

Спеціальні (фахові, предметні):

СК 1. Здатність застосовувати знання та вміння з математики, фізики, хімії та інших суміжних наук для вирішення конкретних біологічних завдань.

СК 2. Здатність демонструвати базові теоретичні знання в галузі біологічних наук та на межі предметних галузей.

СК 5. Здатність до критичного осмислення новітніх розробок у галузі біології і професійній діяльності.

Програмні результати навчання:

ПРН 2. Застосовувати сучасні інформаційні технології, програмні засоби та ресурси Інтернету для інформаційного забезпечення професійної діяльності.

ПРН 6. Застосовувати моделі, методи і дані фізики, хімії, екології, математики у процесі навчання та забезпечення професійної діяльності.

ПРН 20. Аргументувати вибір методів, алгоритмів планування та проведення лабораторних та клініко-лабораторних досліджень, у т.ч. математичних методів та програмного забезпечення для проведення досліджень, обробки та представлення результатів.

Тематичний план лекцій (за модулем) із зазначенням основних питань, що розглядаються на лекції

№ п/п	Назва теми	К-ть годин
Змістовий модуль 1. Комп'ютер у діяльності біолога. Методологія обробки та аналізу інформації.		
1	Інформаційні технології в біології. Медичні дані. Теорія інформації. Вимірювання інформації. Структура інформаційних мереж. Структура глобальної мережі та її доступність до нелегітимного використання. Біомедичні ресурси Інтернету та їх безпечне використання.	2
2	Медичні інформаційні системи. Види медичних інформаційних систем. Локальні і мережеві інформаційні системи. Телемедицина. Електронна система охорони здоров'я в Україні. Захист медичних інформаційних систем.	2
3	Кібератаки. Цілі кібератак. Види загроз. Етичні та юридичні проблеми, пов'язані з нелегітимним доступом до конфіденційних даних. Наслідки та масштаби кібератак в	2

	медичній галузі. Основні заходи протидії кібератакам.	
Разом		6

Тематичний план семінарських занять за модулем і змістовими модулями із зазначенням основних питань, що розглядаються на семінарському занятті – семінарські заняття програмою не передбачено.

Тематичний план практичних занять за модулем і змістовими модулями із зазначенням основних питань, що розглядаються на практичному занятті

№ п/п	Назва теми	К-ть годин
Модуль 1. Основи інформаційних технологій в біології. Основи кібербезпеки. <i>Змістовий модуль 1. Комп'ютер у діяльності біолога. Методологія обробки та аналізу інформації.</i>		
1.	Вхідний контроль. Використання інформаційних технологій в біології. Вимірювання інформації – Застосування комп'ютерів та програмного забезпечення для опрацювання медико-біологічних даних. – Медичні дані, види. Медична інформація, властивості, вимірювання. – Рівні ієрархії інформації – Кодування та декодування інформації. – Інформаційна ентропія та її властивості. – Поняття інформаційних технологій, напрямки розвитку інформаційних технологій у медицині.	2
2.	Медичні інформаційні системи. – Компоненти медичних інформаційних систем. – Користувацькі ролі. – Типи медичних інформаційних систем. – Електронна система охорони здоров'я.	2
3.	Internet технології. Доступ до ресурсів Інтернету. – Інформаційні мережі. Типи мереж. – Характеристики комп'ютерних мереж. – Структура Інтернету. – Ресурси Інтернету. – Адресація в Інтернеті. – Медичні ресурси і Інтернеті та доступ до них. – Структурні методи підтримки безпеки в Інтернеті.	2
4.	Індивідуальні медичні картки. Проблема конфіденційності. – Визначення та цілі ЕМК в сучасній медицині. – Структуризація змісту електронних медичних карток. – Основні складові ЕМК.	2

	<ul style="list-style-type: none"> - Структуризація медичних даних - Стандарти обміну медичною інформацією: HL7, DICOM. - Доступ до електронних медичних карток. - Технології забезпечення доступу та зберігання ЕМК. - Розвиток мобільних додатків для пацієнтів та їх можливості в управлінні власними ЕМК. 	
5.	<p>Види кібератак.</p> <ul style="list-style-type: none"> - Класифікації кібератак. - Шкідливе програмне забезпечення. - Фішинг та соціальна інженерія. - Поширеність кібератак. <p>Заходи кібербезпеки та найкращі практики протидії кібератакам.</p>	2
6.	<p>Кібербезпека.</p> <ul style="list-style-type: none"> - Засади і принципи державної політики у сфері інформаційної безпеки та кібербезпеки. - Закон України «Про захист персональних даних». - Особливості та взаємозв'язок інформаційної безпеки та кібербезпеки. Тріада CIA. - Файли cookies: переваги та недоліки. Безпека та ризики використання соціальних мереж та месенджерів. - Захист аккаунту від зламу: паролі та двофакторна/багатофакторна автентифікація. - Практичні аспекти особистої кібербезпеки. 	2
7.	Підсумковий модульний контроль	2
Разом		14
Самостійна робота		
№	Назва теми	К-ть годин
1.	<p>Етичні та правові принципи в системі охорони здоров'я</p> <ul style="list-style-type: none"> - Захист медичної інформації. - Проблеми впровадження комплексних систем захисту. - Законодавчий контекст щодо захисту медичних даних. - Виявлення загроз та потенційних порушень безпеки даних. - Виклики та перспективи у покращенні захисту медичної інформації. 	5
2.	<p>Системи підтримки прийняття рішень. Експертні системи. Машинне навчання. Вразливості СППР.</p> <ul style="list-style-type: none"> - Системи підтримки прийняття рішень. - Типи медичних знань. Експертні системи (ЕС). - Етапи розробки експертних систем. - Стратегії отримання медичних знань. - База знань експертної системи. 	5

	<ul style="list-style-type: none"> - Застосування експертних систем у медицині. - Машинне навчання - Види машинного навчання. 	
3.	<p>Бази даних для медичних інформаційних систем. Розподілені бази даних. Хмарні технології.</p> <ul style="list-style-type: none"> - Системи управління базами даних (СУБД). - Класифікація систем управління базами даних. - Структура даних. Функції СУБД. - Бази даних в медичних інформаційних системах. - Розподілені бази даних (РБД), їх типи. - Застосування РБД в медичній галузі. - Принципи та ключові характеристики хмарних технологій - Дата-центри. - Хмарні технології в медичній галузі. - Проблеми безпеки даних в контексті ЗБД та хмарних технологій. 	5
4.	<p>Вразливість програм та файлів до зловмисних впливів: структурні передумови.</p> <ul style="list-style-type: none"> - Структурні особливості операційних систем. - Вразливості та методи захисту операційної системи Windows. - Структурні особливості текстових файлів різних типів, їхні вразливості та методи запобігання шкідливим діям. - Метадані. - Файли презентацій, потенційні загрози. - Структурні особливості графічних файлів. Метадані графічних файлів в аспекті кібербезпеки. - Медичні зображення та проблема безпеки персональних даних. 	5
5.	<p>Безпечне використання браузера.</p> <ul style="list-style-type: none"> - Браузери: функції та налаштування. - Аккаунт. - Заходи безпеки у браузері Google Chrome. - Режим перегляду сайту інкогніто. - Менеджер паролів у Google Chrome. - Профілі Chrome. - Керований профіль. - Заходи безпеки у браузері Microsoft Edge. - Режим перегляду сайту <i>InPrivate</i>. - SmartScreen. - Профілі Edge. - Менеджер паролів Edge. - Рекомендації Microsoft для випадків кібератак або підозри кібератаки 	6

6.	<p>Кібербезпека.</p> <ul style="list-style-type: none"> - Засади і принципи державної політики у сфері інформаційної безпеки та кібербезпеки. - Закон України «Про захист персональних даних». - Особливості та взаємозв'язок інформаційної безпеки та кібербезпеки. Тріада CIA. - Файли cookies: переваги та недоліки. Безпека та ризики використання соціальних мереж та месенджерів. - Захист аккаунту від зламу: паролі та двофакторна/багатофакторна автентифікація. - Практичні аспекти особистої кібербезпеки. 	6
7.	<p>Сучасні методи шифрування текстів.</p> <ul style="list-style-type: none"> - Основні принципи - Основи шифрування та дешифрування методом Цезаря - Шифр підстановки - Шифр Віженера - Шифр RSA 	5
8.	<p>Кібербезпека в медицині</p> <ul style="list-style-type: none"> - Захист електронних медичних записів (EMR) - Методи захисту медичних даних. - Використання шифрування для захисту електронних медичних записів. - Кібербезпека телемедицини - Захист даних пацієнтів при наданні телемедичних послуг. - Регулювання та стандарти кібербезпеки в медицині - Вимоги HIPAA та інші регуляторні стандарти. - Впровадження стандартів кібербезпеки в медичних установах. 	6
9.	<p>Кібергігієна</p> <ul style="list-style-type: none"> - Основи кібергігієни. Найкращі практики для захисту персональних пристроїв. - Значення регулярного оновлення програмного забезпечення. - Розпізнавання та уникнення фішинг-атак: ознаки фішинг-атак та способи їх уникнення. - Інструменти для перевірки достовірності електронних листів та вебсайтів. - Створення та управління безпечними паролями, рекомендації. - Безпека в соціальних мережах. захист особистої інформації в соціальних мережах. - Управління налаштуваннями конфіденційності та безпеки. 	6
10.	<p>Використання антивірусних програм та інших засобів</p>	5

	<p>безпеки.</p> <ul style="list-style-type: none"> - Огляд сучасних антивірусних рішень. - Значення антивірусних програм для кібергієни. - Резервне копіювання даних, важливість та методи регулярного резервного копіювання. - Вибір безпечних методів зберігання резервних копій. - Політики та рекомендації для безпечної роботи в офісі. 	
11.	<p>Кібергієна в медицині.</p> <ul style="list-style-type: none"> - Основи кібергієни для медичного персоналу. - Рекомендації для медичного персоналу щодо безпеки в Інтернеті. - Захист персональних даних пацієнтів, важливість кібергієни для захисту особистих даних у медицині. - Методи забезпечення конфіденційності пацієнтів. - Запобігання фішинг-атакам у медичних установах. - Навчання персоналу розпізнавати фішинг-атаки. - Технології для запобігання фішинг-атакам у лікарнях. - Створення та управління безпечними паролями у медичних установах. - Резервне копіювання та відновлення даних у медицині. - Стратегії резервного копіювання медичних даних. - Використання антивірусних програм у медичних системах. - Кібергієна у використанні мобільних пристроїв медичним персоналом. - Захист мобільних пристроїв, що використовуються для роботи з медичними даними. - Безпека при роботі з телемедициною 	6
12.	<p>Новітні проблеми безпеки: штучний інтелект та кібербезпека; квантова криптографія.</p> <ul style="list-style-type: none"> - Штучний інтелект у захисті від кіберзагроз. - Ризики та негативні наслідки застосування штучного інтелекту - Вразливості систем ШІ. - Правові та етичні проблеми застосування ШІ. - Квантові комп'ютери – загроза сучасним паролем та методам шифрування. - Квантова криптографія. 	6
13.	<p>Автоматизація роботи з документами. Електронні форми і бланки медичної документації.</p> <ul style="list-style-type: none"> - Проектування форм. - Створення, редагування електронних форм і бланків. - Захист форм. 	5
14.	<p>Розрахунки в електронних таблицях. Сортування даних та застосування автофільтрів.</p>	6

	<ul style="list-style-type: none"> – Використання формул та функцій для розрахунків. – Використання абсолютних і відносних посилань у формулах. – Сортування даних у таблицях. <p>Фільтрування даних за допомогою автофільтру.</p>	
15.	<p>Оптимізаційні задачі у медицині.</p> <ul style="list-style-type: none"> – Поняття про оптимізаційні задачі. Класифікація задач оптимізації. – Постановка задачі оптимізації. Основні етапи розв'язування оптимізаційних задач. <p>Технологія розв'язування оптимізаційних задач у середовищі табличного процесора.</p>	6
16.	<p>Вирішення задач оптимального керування засобами табличного процесора.</p> <ul style="list-style-type: none"> – Призначення та основні можливості електронних таблиць. Види даних. – Введення, редагування, копіювання і видалення даних. <p>Форматування даних в електронних таблицях.</p>	6
17.	<p>Основи проектування баз даних. Система управління базами даних (СУБД).</p> <ul style="list-style-type: none"> – Поняття бази даних, вимоги до баз даних, їх архітектура. – Етапи розробки баз даних. – Загальна характеристика бази даних. – Основні об'єкти бази даних. – Створення бази даних. – Робота з даними у таблиці. 	6
18.	<p>Розробка моделі бази даних. Створення об'єктів бази даних: форми, фільтри.</p> <ul style="list-style-type: none"> – Загальні відомості про форми та їх створення. – Використання Майстра форм. – Розробка форми у режимі Конструктор. – Підстановка даних. – Застосування фільтра для перегляду вибраних записів у базі даних. 	5
19.	<p>Пошук та аналіз інформації за допомогою запитів. Створення звітів.</p> <ul style="list-style-type: none"> – Призначення та види запитів. – Обчислювальні поля у запитах. – Використання вбудованих функцій. – Звіт як об'єкт бази даних. – Послідовність створення звіту. 	5
20.	<p>Впровадження і використання продуктів Google у біології.</p> <ul style="list-style-type: none"> – Місце хмарних технологій в сучасному світі – Google Диск та пов'язані з ним сервіси. 	5

	– Додаткові сервіси Google	
21.	Візуалізація медико-біологічних даних. Обробка та аналіз медичних зображень. – Радіологічні та нерадіологічні методи отримання медичних зображень; аналогові, матричні зображення. – Методи отримання медичних зображень: рентгенологічний, цифрова ангиографія, комп'ютерна томографія, ядерно-магнітний резонанс, ультразвукове дослідження, сцинтиграфія. – Основні принципи обробки зображень.	5
22.	Кодування та класифікація. Основні принципи класифікації. – Поняття «класифікація» та «кодування». Таксономія, нозологія, нозографія. – Міжнародні системи класифікації. – Класифікаційні системи лікарських препаратів.	5
Разом		120

Індивідуальні завдання – програмою не передбачено

Перелік теоретичних питань для підготовки здобувачів освіти до підсумкового модульного контролю.

1. Поняття «інформація», «дані», «знання».
2. Передача інформації. Визначення кількості інформації.
3. Поняття та визначення інформаційних технологій.
4. Проблеми і перспективи використання інформаційних технологій в біології, охороні здоров'я.
5. Основні поняття комп'ютерних мереж.
6. Класифікація комп'ютерних мереж.
7. Глобальна мережа Internet: протоколи, принцип комутації пакетів, адресація в Internet.
8. Основні способи пошуку інформації, мова пошукових запитів Google.
9. Призначення та основні можливості електронних таблиць. Види даних.
10. Основні поняття: діаграма, графік. Вибір типу діаграми.
11. Поняття системи управління базами даних (СУБД).
12. Основні функціональні можливості СУБД.
13. Етапи розробки баз даних. Об'єкти СУБД: таблиці, форми, запити, звіти.
14. Впровадження і використання продуктів Google у медицині.
15. Місце хмарних технологій в сучасному світі
16. Google Диск та пов'язані з ним сервіси.
17. Поняття «класифікація» та «кодування». Таксономія, нозологія, нозографія.

18. Міжнародні системи класифікації.
19. Системи підтримки прийняття рішень.
20. Експертні системи їх структура та режими роботи.
21. Застосування експертних систем. Засоби прогнозування.
22. Поняття про оптимізаційні задачі. Класифікація задач оптимізації.
23. Візуалізація медико-біологічних даних. Обробка та аналіз медичних зображень.
24. Радіологічні та нерадіологічні методи отримання медичних зображень; аналогові, матричні зображення.
25. Інформаційні системи у медичній галузі.
26. Характеристика та особливості інформаційних ресурсів системи охорони здоров'я.
27. Засади і принципи державної політики у сфері інформаційної безпеки та кібербезпеки.
28. Кібербезпека в медицині. Найкращі практики для захисту персональних пристроїв, електронних медичних записів (EMR).
29. Методи захисту медичних даних.
30. Основи кібергігієни для медичного персоналу. Рекомендації для медичного персоналу щодо безпеки в Інтернеті, з телемедициною.

Перелік практичних навичок до підсумкового модульного контролю.

Модуль 1. Основи інформаційних технологій в біології.

Інтерпретувати основні поняття.

1. Аналізувати роль інформації, комунікації та інформаційних технологій в охороні здоров'я.
2. Демонструвати базові вміння використовувати ресурси Інтернет.
3. Інтерпретувати принципи класифікації та кодування інформації.
4. Демонструвати навички використання статистичних функцій та критеріїв для аналізу даних.
5. Демонструвати вміння представляти умови біологічних задач у формальному вигляді.
6. Аналізувати принципи побудови і функціонування систем підтримки прийняття рішень.
7. Інтерпретувати основні поняття експертних систем.
8. Аналізувати тенденції розвитку систем знань.
9. Демонструвати навички роботи з інформаційними системами.
10. Демонструвати вміння використовувати інформаційні ресурси доказової медицини для пошуку медичної інформації.
11. Демонструвати вміння використовувати захист аккаунту від зламу.
12. Демонструвати вміння використовувати антивірусні програми.
13. Демонструвати вміння використовувати сучасні методи шифрування текстів, методів захисту медичних даних.
14. Демонструвати вміння створювати та управляти безпечними паролями.
15. Демонструвати безпечну роботу в соціальних мережах.

16. Демонструвати вміння управляти налаштуваннями конфіденційності та безпеки при роботі і Internet.
17. Демонструвати вміння використовувати антивірусні програми та інших засоби безпеки.

Форма підсумкового контролю успішності навчання

Підсумковий модульний контроль.

Система поточного та підсумкового контролю

На кожному практичному занятті здійснюється поточний контроль знань відповідно конкретним цілям теми. На практичних заняттях оцінюються теоретична, практична підготовка та СРС (самостійна робота здобувача вищої освіти) як підготовка до аудиторних занять.

Оцінка успішності є інтегрованою (оцінюються всі види роботи здобувача вищої освіти як під час підготовки до заняття, так і під час заняття) за критеріями, які доводяться до відома здобувачів вищої освіти на початку вивчення відповідної дисципліни.

Критерії оцінювання знань здобувачів освіти з дисципліни визначаються згідно стандартизованих узагальнених критеріїв оцінювання знань здобувачів вищої освіти в ПДМУ (Положення про організацію і методику оцінювання навчальної діяльності здобувачів вищої освіти в полтавському державному медичному університеті) (таблиця 1).

Таблиця 1.

Стандартизовані узагальнені критерії оцінювання знань здобувачів вищої освіти в ПДМУ

За 4-бальною шкалою	Оцінка в ЕКТС	Критерії оцінювання
5 (відмінно)	A	Здобувач освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили, володіє не менш ніж 90% знань з теми як під час опитування, та усіх видів контролю.
4 (добре)	B	Здобувач освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартизованих ситуаціях, самостійно виправляє помилки, кількість яких незначна, володіє не менш ніж 85% знань з теми як під час опитування, та усіх видів контролю.
	C	Здобувач освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом науково-педагогічного працівника, в цілому самостійно застосовувати її на практиці, контролювати власну діяльність, виправляти помилки, серед яких є суттєві, добирати аргументи для потвердження думок, володіє не менш ніж 75% знань з теми як під час опитування, та усіх видів контролю.

3 (задовільно)	D	Здобувач освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень з допомогою науково-педагогічного працівника може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих, володіє не менш ніж 65% знань з теми як під час опитування, та усіх видів контролю.
	E	Здобувач освіти володіє навчальним матеріалом на рівні вищому за початковий, значну частину його відтворює на репродуктивному рівні, володіє не менш ніж 60% знань з теми як під час опитування, та усіх видів контролю.
2 (незадовільно)	FX	Здобувач освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину матеріалу, володіє менш ніж 60% знань з теми як по час опитування, та усіх видів контролю.
	F	Здобувач освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, володіє менш ніж 60% знань з теми як під час опитування, та усіх видів контролю.

Конвертація поточної оцінки, виставленої за традиційною 4-бальною шкалою, в багатобальну на кожному занятті не проводиться.

Конвертація оцінки за традиційною 4-бальною шкалою у багатобальну (максимум 120 балів) проводиться лише після поточного заняття, яке передуює підсумковому модульному контролю. Конвертація проводиться за таким алгоритмом:

- підраховується середня оцінка здобувача вищої освіти за традиційною 4-бальною шкалою, отримана протягом поточних занять, що належать до цього модулю (з точністю до сотих балу);
- середній бал поточної успішності розраховується на загальну кількість занять у модулі, а не на фактично відвідану здобувачем вищої освіти;
- для одержання конвертованої багатобальної сумарної оцінки поточної успішності за модуль використовується підрахована середня оцінка за модуль, отримана за традиційною 4-бальною шкалою, помножена на коефіцієнт 24. Винятком є випадок, коли середня за традиційною 4-бальною шкалою оцінка становить 2 бали. У цьому разі здобувач вищої освіти отримує 0 балів за багатобальною шкалою, або для одержання конвертованої багатобальної сумарної оцінки поточної успішності за модуль використовують таблицю 2. 2 (Положення про організацію і методику оцінювання навчальної діяльності здобувачів вищої освіти в полтавському державному медичному університеті).

Мінімальна конвертована сума балів поточної успішності для модуля складає 72 бали.

Таблиця 2

Відповідність середнього балу поточної успішності за традиційною 4-бальною шкалою сумарній оцінці поточної успішності за модуль

Середній бал за поточну успішність (A)	Бали за поточну успішність з модуля (A * 24)	Бали за ПМК з модуля (A*16)	Бали за модуль та/або екзамен (A*24 + A*16)	Категорія ЄКТС	За 4-бальною
--	--	-----------------------------	---	----------------	--------------

2	48	32	80	F FX	2 задовільно
2.1	50	34	84		
2.15	52	34	86		
2.2	53	35	88		
2.25	54	36	90		
2.3	55	37	92		
2.35	56	38	94		
2.4	58	38	96		
2.45	59	39	98		
2.5	60	40	100		
2.55	61	41	102		
2.6	62	42	104		
2.65	64	42	106		
2.7	65	43	108		
2.75	66	44	110		
2.8	67	45	112		
2.85	68	46	114		
2.9	70	46	116		
2.95	71	47	118		
3	72	50	122		
3.05	73	50	123		
3.1	74	50	124		
3.15	76	50	126		
3.2	77	51	128		
3.25	78	52	130	D	
3.3	79	53	132		
3.35	80	54	134		
3.4	82	54	136		
3.45	83	55	138		C
3.5	84	56	140		
3.55	85	57	142		
3.6	86	58	144		
3.65	88	58	146		
3.7	89	59	148		
3.75	90	60	150		
3.8	91	61	152		
3.85	92	62	154		
3.9	94	62	156	B	
3.95	95	63	158		
4	96	64	160		
4.05	97	65	162		
4.1	98	66	164		
4.15	100	66	166		
4.2	101	67	168		
4.25	102	68	170		
4.3	103	69	172		
4.35	104	70	174		

4.4	106	70	176	А	5 ідмінно
4.45	107	71	178		
4.5	108	72	180		
4.55	109	73	182		
4.6	110	74	184		
4.65	112	74	186		
4.7	113	75	188		
4.75	114	76	190		
4.8	115	77	192		
4.85	116	78	194		
4.9	118	78	196		
4.95	119	79	198		
5	120	80	200		

Підсумковий контроль засвоєння модулю відбувається по завершенню вивчення блоку відповідних змістових модулів шляхом тестування та виконання практичних завдань.

До підсумкового модульного контролю допускаються здобувачі вищої освіти, що відвідали всі практичні заняття (або відпрацювали пропущені заняття у встановленому порядку), виконали усі вимоги навчального плану і набрали конвертовану суму балів не меншу за мінімальну – 72 бали. Якщо за результатами поточної успішності здобувач вищої освіти набрав 72 бали, він допускається до складання ПМК.

Наявність оцінки «2» за поточну успішність не позбавляє здобувача вищої освіти права допуску до підсумкового модульного контролю з допустимою мінімальною кількістю балів за поточну успішність.

Здобувач вищої освіти не має право перескладати поточні оцінки «2» якщо він має мінімальну суму балів для допуску до контрольних заходів. Поточні оцінки «3» або «4» не перескладаються. Здобувач вищої освіти зобов'язаний перескладати «2», у разі, якщо середній бал поточної успішності за модуль не досягає мінімального (3,0 бали). Дозвіл на відпрацювання поточної оцінки «2» надає завідувач кафедри лише з метою досягнення здобувачем вищої освіти мінімальної кількості балів для допуску до підсумкового контролю.

Здобувачі вищої освіти які під час вивчення модуля, з якого проводиться підсумковий контроль, мали середній бал поточної успішності від 4,50 до 5,0 звільняються від складання ПМК і автоматично (за згодою) отримують підсумкову оцінку відповідно до таблиці 2, при цьому присутність здобувача освіти на ПМК є обов'язковою. У разі незгоди з оцінкою, зазначена категорія здобувачів вищої освіти складає ПМК за загальними правилами

Оцінювання знань під час проведення ПМК відбувається у два етапи.

Перший – проходження тестового контролю, який містить лише теоретичні питання згідно з програмою дисципліни. Загальна кількість питань у тестовому контролі складає – 25 шт. За кожне питання здобувач освіти має можливість отримати 2 бали. Якщо кількість балів, яку отримав здобувач освіти за тестовий контроль становить більше 20 балів, то тест вважається пройденим

успішно. В іншому випадку вважається тест не пройденим і виставляється загальна незадовільна оцінка за ПМК, яка дорівнює кількості балів правильних відповідей.

Наступний етап – вирішення типових завдань. За вичерпне розв'язання яких здобувач освіти може отримати максимум 30 балів.

Отже, в випадку успішного проходження тесту сумарна оцінка за ПМК складається за схемою:

Загальна оцінка ПМК виставляється відповідно до наступних положень.

ПМК = бали за тестовий контроль + оцінка за завдання

71-80 балів отримує здобувач освіти, який виконав тестові завдання та виявив всебічні, систематичні і глибокі знання, здатність самостійно виконувати завдання, передбачені програмою, ознайомлений з основною і додатковою літературою, рекомендованою програмою. Знання здобувача освіти є міцними, узагальненими; здобувач освіти вміє застосовувати знання творчо, його навчальна діяльність позначена вмінням самостійно оцінювати різноманітні ситуації, явища, факти, виявляти і відстоювати особисту позицію.

61-70 балів отримує здобувач освіти, який виконав тестові завдання та засвоїв навчально-програмовий матеріал у повному обсязі, успішно виконує передбачені програмою завдання, опрацював основну літературу, рекомендовану програмою. Тобто здобувач освіти знає істотні ознаки понять, явищ, закономірностей, зв'язків між ними, а також самостійно застосовує знання в стандартних ситуаціях, володіє розумовими операціями, вміє робити висновки, виправляти допущені помилки. Відповідь повна, правильна, логічна, обґрунтована.

50-60 балів отримує здобувач освіти, який виконав тестові завдання та виявив знання основного навчального матеріалу в обсязі, необхідному для подальшого навчання і майбутньої роботи за професією, здатний виконувати елементарні завдання за зразком, передбачені програмою, ознайомлений з основною літературою, рекомендованою програмою. Як правило, відповідь здобувача освіти при відтворенні навчального матеріалу стисла, зумовлюється початковими уявленнями про предмет вивчення. Здобувач освіти відтворює основний навчальний матеріал та володіє елементарними вміннями навчальної діяльності.

0-49 балів отримує здобувач освіти, який не виконав тестові завдання та у знаннях якого є прогалини, який припустився принципових помилок у виконанні передбачених програмою завдань, тобто здобувач освіти, який неспроможний описати явища, не виявляє знання і розуміння основних положень теми.

У разі порушення здобувачем вищої освіти правил академічної доброчесності (Правила внутрішнього розпорядку для студентів Полтавського державного медичного університету (п.2.2.5)) результати оцінювання, отримані під час складання ПМК, студенту за відповідь виставляється оцінка «незадовільно».

Результат підсумкового модульного контролю оцінюється у балах (традиційна 4-бальна оцінка не виставляється). Максимальна кількість балів підсумкового модульного контролю складає 80 балів. Мінімальна кількість балів підсумкового модульного контролю, за якої контроль вважається складеним, є 50 балів. **Максимальна кількість балів за модуль складає 200 балів** (із них до 120 балів – за поточну успішність).

Методи навчання

Вивчення дисципліни «Цифрові технології в ОЗ. Кібербезпека та кібергігієна» повинно реалізовуватися на основі методів продуктивного навчання, зокрема, проблемного викладу, евристичного, дослідницького, інтерактивного (метод проєктів, моделювання професійних ситуацій, рольові та ділові ігри). При цьому репродуктивні методи повинні використовуватися на початковому етапі навчання, оскільки вони орієнтовані на вміння відтворювати набуті знання щодо вирішення типових завдань шляхом використання алгоритмів, інструкцій, настанов. Особливості методів продуктивного навчання полягають у створенні умов активізації мислення, підвищенні мотивації здобувачів вищої освіти, прийняття творчих рішень, стійкій активності протягом виконання завдань.

Форми та методи оцінювання

- Поточне оцінювання здобувачів освіти на практичних заняття проводиться у формі усного опитування, вирішення ситуаційних завдань, письмового контролю, письмового або програмного комп'ютерного тестування (відповідно до Положення про організацію освітнього процесу в ПДМУ (п. 6 Оцінювання результатів навчання)).
- Підсумковий контроль проводиться у формі модульного контролю (ПМК).

Методичне забезпечення

1. Тематичні плани лекцій та практичних занять.
2. Рекомендована література.
3. Матеріали для контролю знань, умінь і навичок здобувачів освіти: тести різних рівнів складності; ситуаційні задачі; комп'ютерні контролюючі програми.
4. Перелік питань, який повинен засвоїти здобувач вищої освіти при вивченні навчальної дисципліни.

Рекомендована література

Базова

1. Інформаційні технології у медицині: підручник / І.Є. Булах, Л.П. Войтенко, Л.О. Кухар та ін.; за ред. І.Є. Булах. – К. : Медицина, 2008. – 224с.
2. Медична інформатика : навчальний посібник [для здобувач вищої освіти вищих навч. закладів МОЗ України] / О.В. Сілкова, Н.В. Лобач ; МОЗ України, УМСА. – Вид. 2-ге, змін., випр. – Полтава : АСМІ, 2016. – 262 с.
3. Медична інформатика : навчальний посібник для студентів мед. ун-тів / В. Г. Кнігавко, О. В. Зайцева, М. А. Бондаренко та ін. – Харків : ХНМУ, 2020. – 64 с

4. Медична інформатика Частина 1. Електронний навчальний посібник для студ. мед. навч. закл. / Н.В. Лобач, М.С. Саєнко, О.В Сілкова. – Полтава : ПДМУ, 2023. – 257 с.

5. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настродін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с. ISBN 978-617-7844-54-8 <https://jurkniga.ua/contents/osnovi-kiberprostoru-kiberbezpeki-ta-kiberzakhistu.pdf>

Допоміжна

1. Басюк Т.М. Основи інформаційних технологій: навч. посібн. / Т.М. Басюк, Н.О. Думанський, О.В. Пасічник. – Львів : «Новий Світ – 2000», 2020. – 390, с.

2. Журибеда О. Системи керування базами даних : посібник / О. Журибеда. – Київ : Перше вересня, 2017. – 163 с.

3. Інформаційні системи й технології: навч. посіб. для самост. вивч. / Л.М. Симбірська, Г.Д. Симбірський, А.І. Левтеров. – Харків: ХНАДУ, 2016. – 129с.

4. Мережеві організаційні структури управління. Моделювання та візуалізація засобами Excel. / О.Г. Додонов, А.І. Кузьмичов – Київ : Ліра-К, 2021. – 264 с.

5. Пудова, С. С. Медична інформатика : практикум для студентів-медиків / С. С. Пудова, Т. Є. Вуж, Т. Г. Ревіна ; Вінниц. нац. мед. ун-т ім. М. І. Пирогова. – Вінниця : Нілан-ЛТД, 2021. – 103 с.

6. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с. ISBN 978–966–2970–86–9

Інформаційні ресурси

1. www.uacm.kharkov.ua (Українська асоціація «Комп'ютерна Медицина»)
2. <https://www.cochrane.org> (Розділ Кокранівського співтовариства)
3. <https://pubmed.ncbi.nlm.nih.gov/> Національна медична бібліотека (National Library of Medicine)
4. <http://www.compendium.com.ua> (Спеціалізоване медичне інтернет-видання для лікарів, провізорів, фармацевтів, студентів медичних і фармацевтичних ВНЗ)
5. <https://prometheus.org.ua/prometheus-plus/cyber-security-google/> (Безплатне навчання з кібербезпеки від Google та Prometheus)
6. <https://safety.google/intl/uk/cybersecurity-advancements/> (інновації Google у сфері безпеки)
7. <https://www.ndi.org/sites/default/files/%5BUkrainian%5D%20Cybersecurity%20Handbook%20for%20Civil%20Society%20Organizations-compressed.pdf> (Довідник із кібербезпеки для громадянських організацій)
8. <https://wiseit.com.ua/services/hmarni-rishennya/platforma-google-cloud/bezpeka-ta-identyfikacziya/> (Ідентифікація та кібербезпека Google Cloud)

Розробники:

Олена СІЛКОВА – завідувачка кафедрою, кандидат педагогічних наук, доцент.

Лідія КОРОВІНА - кандидат біологічних наук, старший викладач.