СИЛАБУС

Цифрова безпека для освітян

Рівень вищої освіти	другий (магістерський)
Галузь знань	01 Освіта/Педагогіка
Спеціальність	014 Середня освіта
Спеціалізація (за наявності)	-
Освітня програма	-
Вид дисципліни	Вільного вибору
Рік підготовки, семестр	1 рік, 1 семестр
загальна кількість годин/кредитів	90 годин (3 кредити)
Мова викладання	українська

1. ІНФОРМАЦІЯ ПРО ВИКЛАДАЧІВ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПІБ викладача	Москаленко Володимир Валентинович
Кафедра	технологій дистанційного навчання і цифрової дидактики в дошкільній освіті
Посада	доцент
Науковий ступінь	кандидат фізико-математичних наук
Вчене звання	-
Наукові профілі	Google Scholar
Адреса кафедри	вул. Алчевських 29, ауд. 217
Контактна інформація викладача:	voloimir.moskalenko@hnpu.edu.ua

2. ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Політика навчальної дисципліни будується у відповідності до «Положення про організацію освітнього процесу в Харківському національному педагогічному університеті імені Г.С. Сковороди (у новій редакції)» і закріплена Програмою навчальної дисципліни.

Кожен викладач висуває здобувачам вищої освіти систему вимог, правил поведінки студентів на заняттях, взаємин із викладачем, іншими студентами. Вона включає такі базові вимоги:

- не пропускати лекції та семінарські заняття, про відсутність з поважних причин доводити до відома викладача заздалегідь;
- регулярно переглядати лекційний і практичний матеріал;
- здавати й захищати самостійні роботи та завдання у визначені терміни;
- системність і регулярність роботи здобувача вищої освіти з навчальною і науковою літературою;
- обов'язковою є присутність здобувача на модульному та підсумковому контролях.

Здобувач успішно навчається, якщо послідовно набирає кредити, необхідні для здобуття бажаного ступеня. Для цього потрібно, щоб накопичувальний бал був не нижче, ніж 60 за всіма курсами протягом кожного семестру. Якщо накопичувальний бал нижче 60 балів, здобувач вважається неуспішним і може бути відрахований.

Пререквізити навчальної дисципліни	Інформаційно-комунікаційна та математична компетентності рівня першого (бакалаврського) рівня вищої освіти

3. ХАРАКТЕРИСТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Призначення навчальної дисципліни	Призначення навчальної дисципліни: формування цифрового громадянина, фахівця здатного безпечно діяти в цифровому професійному середовищі .
Мета вивчення навчальної дисципліни	формування інформаційно-комунікаційної компетентності Професійного Стандарту (А3), досягнення здобувачами рівня, що відповідає державним та європейським вимогам до ІТ-компетентностей фахівців (DigComp 2.0)
Завдання вивчення навчальної дисципліни	опанування студентами наступних напрямів професійної діяльності: А3131. Основи та принципи медійної грамотності А3132. Юридичні й етичні аспекти використання інформаційно-комунікаційних та цифрових технологій А3231. Типи та функції інформаційно-комунікаційних та цифрових технологій і пристроїв

	А3232. Функціональні особливості, обмеження та наслідки використання інформаційно-комунікаційних та цифрових технологій А3233. Вимоги до організації роботи з технічними засобами навчання; А3331. Ризики і загрози в цифровому середовищі (крадіжки особистих даних, шахрайство, вистежування тощо).
4. РЕЗУЛЬТАТИ НАВЧАННЯ ЗА ДИСЦИПЛІНОЮ * крім ДВВ	
Сформовані програмні компетентності	• Здатність орієнтуватися в інформаційному просторі, здійснювати пошук і критично оцінювати інформацію, оперувати нею у професійній діяльності (А31); • Здатність до використання відкритих ресурсів, інформаційно-комунікаційних та цифрових технологій в освітньому процесі (А32); • Здатність до формування в учнів позитивного ставлення до інформаційно-комунікаційних та цифрових технологій та відповідального їх використання (А33). • Здатність до організації різних форм навчальної і пізнавальної діяльності учнів (Г22).
Програмні результати навчання	• А31У1. Критично оцінювати достовірність, надійність інформаційних джерел, вплив відомостей та інформації на свідомість і розвиток особистості, на прийняття рішень • А31У2. Дотримуватися юридичних і етичних вимог щодо використання інформаційно-комунікаційних та цифрових технологій у педагогічній діяльності • А31У3. Дотримуватися вимог щодо захисту персональних даних та охорони прав інтелектуальної власності • А32У2. Впорядковувати цифрові освітні ресурси і забезпечувати їх доступність для учасників освітнього процесу • А32У4. Організовувати освітній процес з використанням технологій дистанційного навчання. • А33У1. Формувати в учнів критичне ставлення до інформаційно-комунікаційних та цифрових технологій, враховуючи можливості підвищення ефективності навчальної діяльності • А33У2. Розвивати в учнів відповідальність і навички безпечного використання цифрових технологій і сервісів. • Г22У2. Застосовувати індивідуальну, групову, парну і колективну форми організації навчання, з використанням інформаційно-комунікаційних і цифрових технологій
5. СФЕРИ ЗАСТОСУВАННЯ ЗДОБУТИХ НАВИЧОК	
Використання ІТ у професійній діяльності.	
6. МЕТОДИ НАВЧАННЯ	
словесні методи (лекція, дискусія, співбесіда, інструктаж тощо); практичні методи (лабораторні та практичні заняття); відеометод у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані тощо); самостійна робота (розв’язання задач, виконання завдань).	

7. ЗМІСТ ТА ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назва теми/розділу дисципліни	Лекції	Практичні заняття	Лабораторні заняття	Самостійна робота
Модуль 1. Особиста безпека при дистанційному навчанні				
Тема 1.1. Здоров’язбережувальний аспект безпеки	1	2		9

Тема 1.2. Цифровий аспект безпеки	1	2		9
Тема 1.3. Суспільний аспект безпеки	1	4		9
Тема 1.4. Мережевий аспект безпеки	1	2		9
Усього годин за модуль	**4**	**10**		**36**
Модуль 2. Інформаційна безпека в освіті. Медіаграмотність. Кібербезпека.				
Тема 2.1. Мережеві технології та інформаційна безпека.	2	4		4
Тема 2.2. Медіабезпека	2	4		4
Тема 2.3. Кібербезпека	2	2		6
Усього годин за модуль	**6**	**10**		**14**
ІНДЗ				10
Усього:	**10**	**20**		**60**

8. КОНТРОЛЬ І ОЦІНКА РЕЗУЛЬТАТІВ НАВЧАННЯ

Методика оцінювання ґрунтується на принципах об'єктивності, прозорості, гнучкості та високої диференціації.

Шкала оцінювання здобувачів за системою ECTS

Рейтингова оцінка	Оцінка за стобальною шкалою	Значення оцінки
A	90 – 100 балів	Відмінно – відмінний рівень знань (умінь) в межах обов'язкового матеріалу з можливими незначними недоліками
B	82 – 89 балів	Дуже добре – достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	74 – 81 балів	Добре – в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69 – 73 балів	Задовільно – посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60 – 68 балів	Достатньо – мінімально можливий допустимий рівень балів знань (умінь)
FX	35 – 59 балів	Незадовільно з можливістю повторного складання – незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1 – 34 балів	Незадовільно з обов'язковим повторним вивченням курсу – досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни
ФОРМА КОНТРОЛЮ		залік

Розподіл рейтингових балів за видами контролю

Назва виду діяльності та форми контролю	Максимальна кількість балів за одиницю	Кількість одиниць	Максимальна кількість балів за вид роботи
Відвідування лекцій	-		
Підготовка та робота на семінарському занятті	-		
Робота на практичному занятті	5	10	50
Лабораторна робота (в тому числі допуск, виконання, захист)	-		
Виконання завдань для самостійної роботи	5	8	40
Модульний контроль	-		
Виконання і захист ІНДЗ	-		10
Максимальна кількість балів протягом семестру:			100

9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА ТА ІНФОРМАЦІЙНІ ДЖЕРЕЛА

Базова

1. Інформатика : підруч. для 9 кл. загальноосвіт. навч. закл. / [О.О. Бондаренко, В.В.Ластовецький, О.П.Пилипчук, Є.А.Шестопалов]. — Харків : Вид-во «Ранок», 2017.
2. Закон України Про кібернетичну безпеку України
3. Закон України Про електронний підпис.
4. Д. Золотухін: Посилення кібербезпеки залежить від розвитку освіти в цій сфері

Допоміжна

1. http://udcpo.com.ua/cybersafety_in_educational_institutions/
2. http://udcpo.com.ua/cybersafety_in_educational_institutions/
3. http://www.moneyweek.com.ua/wp-content/uploads/2014/02/GMW-Safety.pdf
4. https://www.mba-magistratura.com/Master/%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0/%D0%86%D1%82%D0%B0%D0%BB/

Інформаційні ресурси

1. https://high.itstep.org/2017/02/19/kompyuterni-merezhi-ta-kiberbezpeka/
2. http://www.osvita.org.ua/news/78070.html
3. https://kfund-media.com/kiberbezpeka-v-2018-ataky-cherez-insajderiv-i-tayemnyj-majning/
4. https://nv.ua/ukr/techno/it-industry/telemeditsina-sonjachna-enerhetika-kiberbezpeka-ta-blokchejn-najjaskravishi-startapi-ukrajini-2017-roku-2442340.html
5. http://www.oblosvita.te.ua/news/pozashkilna-osvita/2841-kiberbezpeka-bezpechnyi-internet-dlia-dytyny
6. http://profspilka.kiev.ua/publikacii/novyny/4465-kberbezpeka-ukrayinskih-nuo-zagrozi-ta-yih-podolannya.html
7. http://www.polradio.pl/5/38/Artykul/329565з екрану.