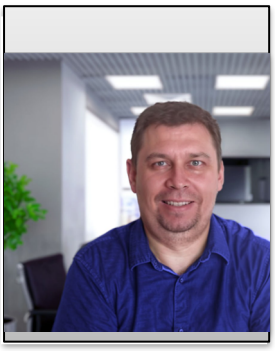
ЗАПОРІЗЬКА ПОЛІТЕХНІКА
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет **Бізнес-технологій та економіки**
Кафедра **Цифрові технології в бізнесі та економіці**

СИЛАБУС
навчальної дисципліни (вибіркова)
ЦИФРОВА ГІГІЄНА
Обсяг освітнього компоненту 4/120 (кредитів/годин)

Освітня програма «Цифрова економіка та електронний бізнес»
Першого рівня вищої освіти
Спеціальність – 051 «Економіка»

ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА



Морозов Денис Миколайович,
кандидат технічних наук,
доцент кафедри цифрових технологій в бізнесі та економіці

Контактна інформація:
- +38(061) -7698504;
-ajax3101@gmail.com ;
- IV навчальний корпус, ауд. 396

Час і місце проведення консультацій:
за графіком консультацій

ОПИС КУРСУ

У курсі «Цифрова гігієна» розглядаються теоретичні засади та практичні аспекти безпечного й відповідального використання цифрових технологій у сучасному інформаційному суспільстві. Дисципліна формує у студентів комплексне розуміння взаємозв'язку між використанням цифрових пристроїв та фізичним, психічним і соціальним благополуччям. Основна увага приділяється розвитку практичних навичок захисту персональних даних, розпізнавання цифрових загроз та створення безпечного цифрового середовища.

Студенти опановують методи аналізу ризиків у цифровому просторі, вивчають стратегії протидії кіберзагрозам та етичні норми поведінки у віртуальному середовищі. Значна частина курсу присвячена питанням профілактики негативного впливу цифрових технологій на здоров'я, формуванню здорових цифрових звичок та балансу між онлайн і офлайн активностями.

Курс має прикладну спрямованість та формує у студентів компетентності щодо: ефективного захисту особистої інформації; організації ергономічного робочого простору при роботі з гаджетами; розпізнавання та протидії маніпуляціям у цифровому середовищі; дотримання принципів цифрової етики; свідомого та збалансованого використання цифрових технологій.

Особливістю курсу є його міждисциплінарний характер, що поєднує елементи інформаційної безпеки, психології, ергономіки та етики, а також орієнтація на формування критичного мислення та навичок самозахисту в цифровому просторі. Це дозволяє студентам отримати актуальні компетентності, необхідні для безпечного та відповідального функціонування в умовах стрімкого розвитку цифрових технологій.

Отримані знання та навички стануть основою для подальшого професійного розвитку в будь-якій сфері, де використовуються сучасні інформаційні технології, сприятимуть підвищенню особистої цифрової стійкості та якості життя в цифрову епоху..

МЕТА, КОМПЕТЕНТНОСТІ ТА РЕЗУЛЬТАТИ НАВЧАННЯ

1. Метою вивчення дисципліни є формування у здобувачів вищої освіти теоретичних знань та практичних навичок безпечного використання цифрових технологій, розвиток критичного мислення щодо оцінки ризиків цифрового середовища, опанування методів захисту персональних даних та забезпечення інформаційної безпеки, а також формування компетентностей щодо зменшення негативного впливу цифрових пристроїв на фізичне та психічне здоров'я, дотримання етичних норм у віртуальному просторі та створення збалансованих цифрових звичок для підвищення якості життя в умовах інформаційного суспільства.

2. Компетентності

Загальні компетентності:

Здатність до критичного мислення, аналізу та оцінки інформації в цифровому просторі.

Здатність вчитися і оволодівати сучасними знаннями у сфері інформаційної безпеки та цифрових технологій.

Знання та розуміння принципів безпечної та етичної поведінки в цифровому середовищі.

Здатність застосовувати знання у практичних ситуаціях, пов'язаних із захистом персональних даних та протидією цифровим загрозам.

Навички використання сучасних інструментів захисту інформації та цифрової приватності.

Здатність до самоорганізації та формування здорових цифрових звичок.

Здатність приймати обґрунтовані рішення щодо використання цифрових технологій з урахуванням їх впливу на фізичне та психічне здоров'я.

Фахові компетентності:

Здатність застосовувати теоретичні знання з цифрової гігієни для аналізу ризиків та загроз цифрового середовища.

Здатність використовувати інструменти захисту персональних даних та забезпечення конфіденційності в мережі Інтернет.

Здатність аналізувати та протидіяти соціальній інженерії, фішингу та іншим методам маніпуляції в цифровому просторі.

Здатність організовувати ергономічне робоче середовище при роботі з цифровими пристроями для мінімізації негативного впливу на здоров'я.

Здатність ідентифікувати та протидіяти цифровій залежності, інформаційному перевантаженню та професійному вигоранню.

Здатність дотримуватись етичних норм та правових аспектів використання цифрових технологій.

Здатність впроваджувати стратегії цифрового добробуту для балансування онлайн і офлайн активностей.

Здатність розробляти та реалізовувати індивідуальні та організаційні заходи з підвищення цифрової стійкості та інформаційної безпеки.

3. Очікувані програмні результати навчання:

Аналізувати та оцінювати ризики в цифровому середовищі, ідентифікувати потенційні загрози інформаційній безпеці та приватності.

Використовувати сучасні інструменти захисту персональних даних, включаючи менеджери паролів, двофакторну автентифікацію та шифрування даних.

Розпізнавати та протидіяти методам соціальної інженерії, фішингу, шахрайським схемам та маніпуляціям у цифровому просторі.

Організовувати ергономічне робоче середовище при роботі з цифровими пристроями для мінімізації негативного впливу на зір, опорно-руховий апарат та загальний фізичний стан.

Впроваджувати стратегії цифрового добробуту для балансування онлайн і офлайн активностей, запобігання цифровій залежності та інформаційному перевантаженню.

Застосовувати методи захисту від небажаного контенту, кібербулінгу та інших форм цифрового насильства.

Дотримуватись етичних норм та правових аспектів використання цифрових технологій, включаючи авторське право, інтелектуальну власність та захист персональних даних.

Розвивати навички критичного мислення для оцінки достовірності інформації, виявлення дезінформації та маніпуляцій у цифровому середовищі.

Розробляти та реалізовувати індивідуальні стратегії цифрової гігієни для підвищення якості життя в умовах інформаційного суспільства.

ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ ДИСЦИПЛІНИ

Передумовами для вивчення дисципліни «Цифрова гігієна» є наявність у здобувачів вищої освіти базових навичок роботи з комп'ютером та мобільними пристроями, а також елементарних знань з інформаційних технологій, отриманих під час попереднього навчання. Студенти повинні володіти основами користування інтернетом, соціальними мережами та месенджерами, а також розуміти загальні принципи функціонування цифрових пристроїв та онлайн-сервісів. Також важливими передумовами є: здатність до критичного мислення та аналізу інформації; базове розуміння концепцій інформаційної безпеки та приватності; усвідомлення потенційних ризиків у цифровому середовищі; вміння працювати з базовими налаштуваннями приватності на цифрових пристроях та в онлайн-сервісах; навички пошуку та оцінки достовірності інформації в інтернеті; здатність до самоорганізації та розвитку особистої цифрової компетентності. Вивчення дисципліни не потребує глибоких технічних знань або навичок програмування, проте передбачає зацікавленість студентів у питаннях безпечного та відповідального використання цифрових технологій, а також їхню готовність адаптувати власні цифрові звички відповідно до принципів цифрової гігієни.

ПЕРЕЛІК ТЕМ (ТЕМАТИЧНИЙ ПЛАН) ДИСЦИПЛІНИ

Таблиця 1 – Загальний тематичний план аудиторної роботи

Номер тижня	Теми лекцій, год.	Теми практичних робіт, год.
1	2	3
Змістовий модуль 1 Основи цифрової гігієни та безпеки в цифровому просторі		
1	Вступ до цифрової гігієни: поняття, актуальність та значення (2 год)	Аналіз власного цифрового сліду та аудит цифрових звичок (2 год)

2	Інформаційна безпека: основні принципи захисту персональних даних (2 год)	Налаштування приватності в соціальних мережах та онлайн-сервісах (2 год)
3	Управління паролями та методи автентифікації (2 год)	Використання менеджерів паролів та налаштування двофакторної автентифікації (2 год)
4	Загрози в цифровому просторі: фішинг, соціальна інженерія, шкідливе ПЗ (2 год)	Аналіз та розпізнавання фішингових атак та методів соціальної інженерії (2 год)
5	Безпечне користування мобільними пристроями та публічними мережами (2 год)	Налаштування безпеки мобільних пристроїв та захист при використанні публічних Wi-Fi (2 год)
6	Фізична гігієна в цифровому середовищі: ергономіка та організація робочого простору (2 год)	Оцінка та оптимізація ергономіки робочого місця, налаштування освітлення та дисплеїв (2 год)
7	Вплив цифрових пристроїв на зір та опорно-руховий апарат (2 год)	Практичні вправи для зменшення навантаження на зір та опорно-руховий апарат (2 год)
Змістовий модуль 2 Психологічна цифрова гігієна та етичні аспекти використання цифрових технологій		
8	Психологічна гігієна в цифровому середовищі: цифрове перевантаження та інформаційний стрес (2 год)	Методики управління потоком інформації та зменшення цифрового перевантаження (2 год)
9	Цифрова залежність: причини, наслідки та профілактика (2 год)	Розробка персональної стратегії балансу онлайн і офлайн активностей (2 год)
10	Цифрові звички та їх вплив на здоров'я: сон, активність, концентрація уваги (2 год)	Аналіз та оптимізація власних цифрових звичок для підвищення продуктивності (2 год)
11	Етика та права у цифровому світі: авторські права, інтелектуальна власність (2 год)	Практикум з етичного використання та цитування цифрових матеріалів (2 год)
12	Кібербулінг та інші форми цифрового насильства: розпізнавання та протидія (2 год)	Кейс-стаді з розпізнавання та протидії кібербулінгу (2 год)
13	Критичне мислення та медіаграмотність у цифровому просторі (2 год)	Практикум з перевірки достовірності інформації та виявлення фейків (2 год)
14	Цифрова гігієна в професійному середовищі. Підсумкове заняття (2 год)	Розробка комплексної стратегії цифрової гігієни. Підсумкове оцінювання (2 год)

САМОСТІЙНА РОБОТА

1. Опрацювання лекційних матеріалів та конспектування ключових понять цифрової гігієни.

2. Вивчення додаткових джерел (статей, підручників, електронних ресурсів) щодо інформаційної безпеки, захисту персональних даних та впливу цифрових технологій на здоров'я.
3. Аналіз актуальних тенденцій у сфері кіберзагроз та методів протидії їм (фішинг, соціальна інженерія, шкідливе ПЗ).
4. Вивчення сучасних стандартів та рекомендацій з інформаційної безпеки (наприклад, GDPR, стандарти шифрування даних, рекомендації з безпечного використання паролів).
5. Підготовка рефератів або аналітичних оглядів з актуальних тем (наприклад, "Вплив соціальних мереж на психологічне здоров'я", "Сучасні методи цифрової маніпуляції", "Ергономіка цифрового робочого простору").
6. Вивчення методів захисту від цифрового перевантаження та стратегій цифрового добробуту в різних сферах життя.
7. Ознайомлення з правовими аспектами використання цифрових технологій (авторське право, інтелектуальна власність, захист персональних даних).
8. Дослідження впливу гаджетів на фізичне здоров'я та вивчення ергономічних рекомендацій для роботи з цифровими пристроями.
9. Аналіз власних цифрових звичок та розробка плану їх оптимізації згідно з принципами цифрової гігієни.
10. Моніторинг та аналіз новин у сфері цифрової безпеки, вивчення актуальних кіберзагроз та методів їх уникнення.

РЕКОМЕНДОВАНІ ІНФОРМАЦІЙНІ ТА НАВЧАЛЬНО-МЕТОДИЧНІ ДЖЕРЕЛА

Літературні джерела:

1. Цифрова гігієна: підручник – Київ: ІВЦ «Видавництво «Політехніка», 2023.
2. Захист персональних даних: навчальний посібник – Вінниця: ВНТУ, 2022.
3. Етика в Інтернеті: практичний посібник – Київ: «Кондор», 2021.
4. Digital Hygiene: A Guide to Safe and Responsible Technology Use – Oxford University Press, 2022.
5. Cybersecurity for Beginners – Wiley, 2023.
6. The Psychology of Social Media: From Brain to Culture – Cambridge University Press, 2021.

ОЦІНЮВАННЯ

Методами контролю є: усний контроль (усне опитування), письмовий, тестовий контроль, а також методи самоконтролю і самооцінки.

Система контролю знань здобувачів вищої освіти з дисципліни «Цифрова гігієна» включає в себе:

- поточний контроль;
- підсумковий контроль.

Поточний контроль знань здійснюється на практичних заняттях за допомогою усного або письмового опитування. Основне завдання поточного контролю – перевірка рівня підготовки здобувачів вищої освіти до виконання конкретної роботи.

Об'єктами поточного контролю знань здобувачів вищої освіти з дисципліни «Цифрова гігієна» є:

- систематичність та активність роботи на заняттях;
- виконання обов’язкових завдань практичної роботи;
- виконання контрольної роботи.

Результати поточного контролю (поточна успішність) є основною інформацією під час проведення заліку і враховуються викладачем при визначенні підсумкової оцінки з дисципліни.

Підсумковий контроль з дисципліни проводиться з метою оцінювання результатів навчання на певному освітньому ступені або на окремих його завершених етапах за 100-бальною системою.

Контроль з дисципліни «Цифрова гігієна» проводиться у восьмому семестрі у формі заліку в обсязі навчального матеріалу, визначеного програмою навчальної дисципліни, і в терміни, встановлені робочим навчальним планом, індивідуальним навчальним планом здобувача вищої освіти.

Студенти заочної форми навчання виконують контрольну роботу. Після перевірки викладачем контрольної роботи і одержання позитивної оцінки студента отримує залік.

Згідно з діючою в університеті системою комплексної діагностики знань студентів, з метою стимулювання планомірної та систематичної навчальної роботи, оцінка знань студентів здійснюється за 100-бальною системою.

Протягом семестру студент проходить два поточних контролі у вигляді контрольної роботи, кожний з яких оцінюється за 10-бальною шкалою. Студент отримує підсумкову оцінку по дисципліні за результатами поточної роботи. В 100-бальну оцінку входять поточний контроль (100 балів).

Підсумкова оцінка із дисципліни, яка виставляється в залікову відомість є сумою балів за різні види навчальної роботи.

Поточне тестування та самостійна робота				Сума
МОДУЛЬ 1		МОДУЛЬ 2		
Змістовий модуль 1	КР	Змістовий модуль 2	КР	
30	15	40	15	100

КР – контрольна робота

ПОЛІТИКИ КУРСУ

Під час навчання студенти зобов'язані дотримуватися академічної доброчесності:

- самостійно виконувати лабораторні роботи, завдання поточного та підсумкового контролю;
- дотримуватися норм законодавства про авторське право;
- приймати активну участь у навчальному процесі;
- не запізнюватися на заняття, не пропускати заняття без поважних причин;
- самостійно і своєчасно вивчати матеріал пропущеного заняття;
- давати достовірну інформацію про результати власної навчальної діяльності.
- бути терпимим і доброзичливим до однокурсників та викладачів.
- при вивченні курсу політика дотримання академічної доброчесності визначається Кодексом академічної доброчесності Національного університету «Запорізька політехніка» https://zp.edu.ua/uploads/dept_nm/Nakaz_N253_vid_29.06.21.pdf

ТЕХНІЧНІ ВИМОГИ ДЛЯ РОБОТИ НА КУРСІ

Щоб мати доступ до навчально-методичних розробок курсу необхідно мати особистий доступ до університетської навчальної платформи Moodle.