АНОТАЦІЯ КУРСУ

1. Викладач:

1.1. Лектор:

Костюк Юлія Володимирівна

- *вчене звання та посада:* старший викладач кафедри інженерії програмного забезпечення та кібербезпеки;
- *контактиний телефон*: (044)-513-98-62, (044)-531-49-57;
- *e-mail:* kostyuk_yu@knute.edu.ua
- *наукові інтереси:* новітні інформаційні технології, хмарні технології, технології дистанційного навчання, кібербезпека інформаційних технологій,
- *стажування та підвищення кваліфікації:* Державний університет телекомунікацій (м. Київ, в період з 23 листопада 2020р. по 04 грудня 2020р., курс «Системи технічного захисту інформації» з обсягом навчального часу 120 годин/ чотири кредита ЄКТС). (сертифікат №СТ38855350/111-20).

Підвищення кваліфікації.

National Research University Higher School of Economics, на Coursera «Методы и средства защиты информации». Виданий 08.08.2020р. ***IPD Week, October 2020 hosted by the Technical Field Engagement Team 5 - 9 October 2020.***

Cisco Networking Academy. Сертифікати: **Introduction to Packet Tracer**, виданий 27.07.2020;, **Introduction to IoT**, виданий 22.01.2021. **Introduction to IoT**. виданий 22.01.2021р.; **Academy Orientation,** виданий 19.02.2021 р.

Cisco Grant Instructor Training.STEM center Socrat.

CCNAv7: Introduction to Networks, сертифікат виданий 20.02.2021 р.

Academy Orientation, виданий 19.02.2021 р.

Networking Essential, виданий 21.04.2021р.

Cybersecurity Essentials, виданий 25.04.2021р.

Introduction to Cybersecurity, виданий 26.04.2021р.

Teachers Internship від **EPAM University Programs** з 12.07-4.08.2021р.

Курс **«Про штучний інтелект простими словами» від Школа IT-професіоналів "ProfIT"**.

Науково-практичний курс серії вебінарів компанії **Linkos Group** «Інформаційні технології в економіці: інноваційні рішення захисту даних підприємства» в обсязі 180 год. №IT002 26.05.2021р.

Сертифікати: Цифрові комунікації в глобальному просторі (Prometheus), 13.07.2020р.; Основи інформаційної безпеки

(Prometheus), 19.07.2020р.; The Science of Cybersecurity: Best Practices in the New Normal, 31.10.2020р.; Онлайн-тренінг від ТОВ «Дінтернал Ед'юкейшн» Міжнародна сертифікація викладачів від компанії Майкрософт – не мрія, а реальність, 14.09.2020р.(Серія №DE-32-1409202017-12270); Онлайн-тренінг від ТОВ «Дінтернал Ед'юкейшн» Лайфхаки для роботи з Microsoft Office та переваги сертифікації Microsoft Office Specialist, 14.12.2020р.; Сервисы Google для онлайн – преподавателя, 15.01.2020р.;

2. Обсяг дисципліни: «Організація комп'ютерних мереж»,

- рік навчання: II;
- семестр навчання: 4;
- кількість кредитів: 6;
- кількість годин за семестр: 180 год.
  - лекційних: 24 год.
  - лабораторних: 24 год.
  - на самостійне опрацювання: 132 год.
- кількість аудиторних годин на тиждень:
  - лекційних: 2 год.
  - лабораторних: 2 год.

Всього годин / кредитів ЄКТС	Аудиторні заняття, год		Самостійна робота	Вид підсумкового контролю
	Лекції	Лабораторні роботи		
180 / 6	24	24	132	Іспит

3. Час та місце проведення:

– лекційні заняття - відповідно до розкладу ДТЕУ з врахуванням специфіки дисципліни проведення останньої передбачено в аудиторіях: 510, 510а, 514 або проведення on-line в Microsoft Teams;

– позааудиторна робота - самостійна робота студента, результат виконання якої висвітлено засобами Office 365;

– всі лабораторні завдання виконуються на основі інтерактивних методів навчання у електронному середовищі.

ДОВІДКОВА ІНФОРМАЦІЯ

Кафедра інженерії програмного забезпечення та кібербезпеки	тел. 15-71, progen@knute.edu.ua, кабінет Б-502

Завідувач кафедри – д.т.н., проф. Криворучко О. В.	тел. 15-70, kryvoruchko_ev@knute.edu.ua, кабінет Б-502
Дні занять	за розкладом
Консультації	за розкладом або on-line
Мова викладання	українська

4. Пререквізити та постреквізити навчальної дисципліни:

- **пререквізити:** дисципліна базується на знаннях та компетентностях, що набуває здобувач вищої освіти під час вивчення дисциплін «Інформаційних технологій в професійній діяльності», «Іноземної мови за професійним спрямуванням»
- **постреквізити:** дисципліна надає студентам необхідні знання та навички, які будуть корисні при вивченні дисциплін «Інформаційні війни», при проходженні виробничої практики, підготовці до випускного кваліфікаційного проекту, у подальшій професійній діяльності.

5. Результати вивчення дисципліни:

Номер в освітній програмі	Зміст компетентності
Загальні компетентності за освітньою програмою	
ЗК3	Навички використання інформаційних і комунікаційних технологій
ЗК4	Здатність вчитися і оволодівати сучасними знаннями
ЗК10	Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні
Фахові компетентності за освітньою програмою	
СК3	Здатність до розуміння природи поведінки, діяльності та вчинків
СК10	Здатність дотримуватися норм професійної етики
Програмні результати навчання за освітньою програмою	
ПР3	Здійснювати пошук інформації з різних джерел, у т.ч. з використанням інформаційно-комунікаційних технологій, для вирішення професійних завдань
ПР13	Взаємодіяти, вступати у комунікацію, бути зрозумілим, толерантно ставитися до осіб, що мають інші культуральні чи гендерно-вікові відмінності

6. Характеристика дисципліни:

6.1. <u>Призначення навчальної дисципліни:</u> Дисципліна «Основи кібербезпеки» є вибірковою компонентою навчального плану підготовки студентів денної форми навчання першого (бакалаврського) рівня вищої освіти за спеціальністю 053 «Психологія», галузі знань 05 «Соціальні та поведінкові науки», освітня програма «Практична психологія».

6.2. <u>Мета вивчення дисципліни</u> «Основи кібербезпеки» є формування у майбутніх фахівців необхідного рівня знань щодо правильного поводження з інформацією у кіберсфері та безпечної роботи із засобами комп'ютерної техніки в професійній діяльності; дізнатись про основні загрози в сучасному інформаційному просторі; аналізувати поширені помилки користувачів та наслідки від атак зловмисників і кібершахраїв;
вивчити базові правила захисту інформації на персональних електронних пристроях та в соціальних мережах; навчитись визначати фейкові новини; опанувати основні рекомендації щодо захисту власних даних, безпечного користування електронними пристроями та інформаційними ресурсами.

6.3. <u>Задачі вивчення дисципліни:</u> вивчення дисципліни «Основи кібербезпеки» є засвоєння студентами:

- ✓ знання основних положень, термінів та заходів, що стосуються кібергігієни на робочу місці;
- ✓ знання основної нормативно-правової бази у сфері кібербезпеки та інформаційної безпеки;
- ✓ знання особливостей кібергігієни в системі публічної служби.
- ✓ уміння визначати заходи кібергігієни для конкретної ситуації;
- ✓ уміння оцінювати загрози та вживати заходів реагування на робочому місці;
- ✓ уміння безпечно поводитись у кіберсфері.
- ✓ навички організації безпечного доступу до пристроїв і програм;
- ✓ навички правильного налаштування програмного забезпечення на робочому місці;
- ✓ навички критичного оцінювання інформації;
- ✓ знати різні типи зловмисного ПЗ (відомого як шкідливі програми) та їх симптоми; знати різні методи, якими нападники можуть проникнути в систему: соціальна інженерія, злам паролю Wi-Fi, фішинг та використання вразливостей, тощо.

.

6.4. <u>Зміст навчальної дисципліни:</u> відповідає навчальній та робочій програмі, яка відповідає запитам стейкхолдерів.

6.5. <u>План вивчення дисципліни:</u>

Схема вивчення дисципліни (лекційні заняття)

Тема лекційного заняття	Завдання	Матеріали
1	2	3
ТЕМА 1. КІБЕРПРОСТІР І КІБЕРБЕЗПЕКА — ГОЛОВНІ ОЗНАКИ НОВОЇ ІНФОРМАЦІЙНОЇ ЦИВІЛІЗАЦІЇ **Лекція №1** ***Кіберпростір і кібербезпека — головні ознаки нової інформаційної цивілізації.*** *План лекції №1* 1. Поняття інформаційна безпека, кібербезпека, кіберпростір, кіберборотьба, кібертероризм, кіберзброя**.** 2. Кіберпростір: визначення, система відношень, загрози. Потреба в кібербезпеці. 3. Кіберінциденти: передумови скоєння та наслідки. 4. Поняття «кібервійни». Захист даних та конфіденційності в професійній діяльності психолога. 5. Огляд областей кібербезпеки. Приклади доменів кібербезпеки. 6. Поняття «кіберзлочинець» та мотиви кіберзлочинів. Класифікація зловмисників. **Список рекомендованих джерел:** *Основний: 1[с. 50-59, 66-98, 257-268, 310-312], 2 [с. 7-43], 3 [с. 27-38, 130-146], 4 [с. 112-120].* *Додатковий: 6 [с. 25-28, 172-176, 239, 249-252, 255-263].* *Інтернет-ресурси: 14.*	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)
ТЕМА 2. НАЦІОНАЛЬНА СИСТЕМА КІБЕРБЕЗПЕКИ УКРАЇНИ **Лекція №2** **Національна система кібербезпеки України** *План лекції №2* 1. Національна безпека України: реалії та перспективи. Роль та місце кібернетичної безпеки у загальній системі нацбезпеки. 2. Основні положення Стратегії кібербезпеки України. 3. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці. 4. Правове забезпечення у сфері інформаційної безпеки та кібербезпеки. **Список рекомендованих джерел:**	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)

Тема лекційного заняття	Завдання	Матеріали
1	2	3
Основний: 1 [с. 135-149], 2 [с. 7-24], 3 [с. 222-240], 4 [с. 137-138]. *Додатковий: 6 [с. 189-209], 7 [с. 93-106], 10, 11, 12.* *Інтернет-ресурси: 14, 16.*		
ТЕМА 3. СУТНІСТЬ ТА ОСНОВНІ ПРОЦЕДУРИ КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ **Лекція №3** **Сутність та основні процедури керування кібербезпекою** *План лекції №3* 1. Модель кібербезпеки ISO. 2. Куб кібербезпеки. 2. Захист конфіденційності даних в професійній діяльності психолога. Керування доступом. 3. Потреба в цілісності даних. Перевірка цілісності. 4. Принцип доступності. П'ять дев'яток. Забезпечення доступності. 5. Проблеми захисту збережених даних. Методи передачі даних. Проблеми захисту даних у процесі обробці в професійній діяльності. ***Список рекомендованих джерел:*** *Основний: 1 [с. 54-59], 3 [с. 157-166].* *Додатковий: 6 [с. 218-219].* *Інтернет-ресурси: 14, 15, 16.*	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)
ТЕМА 4. КІБЕРАТАКИ, ЗАГРОЗИ ТА ЇХ ВЛАСТИВОСТІ. ХАРАКТЕРИСТИКА СУЧАСНИХ КІБЕРАТАК **Лекція №4** **Кібератаки, загрози та їх властивості. Характеристика сучасних кібератак** *План лекції №4* 1. Сутність та класифікація кібератак. Етапи реалізації атак. 2. Атаки на бездротові мережі та мобільні пристрої. Атаки на WEP та WPA. 3. Атаки на застосунки. Міжсайтовий скриптинг. Ін'єкція коду. Переповнення буфера. Віддалений запуск програм. 4. Атака "Відмова в обслуговуванні" (DoS). Розподілена DoS атака (Distributed DoS Attack, DDoS).	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)

Тема лекційного заняття	Завдання	Матеріали
1	2	3
5. Зміст, класифікація та ознаки кіберзагроз. Основні характеристики кіберзагроз. Поширення кіберзагроз. Кіберзагрози підвищеної складності. **Список рекомендованих джерел:** *Основний: 2-4* *Додатковий: 5-6, 8* *Інтернет-ресурси: 9, 10*		
ТЕМА 5. ДЕЗІНФОРМАЦІЯ ЯК ЕЛЕМЕНТ КІБЕРАТАК. СЦЕНАРІЇ РОЗВИТКУ ТА МЕТОДИ ПРОТИДІЇ **Лекція №5** Дезінформація як елемент кібератак. Сценарії розвитку та методи протидії ***План лекції №5*** 1. Канали поширення дезінформації. Типи неправдивої інформації в професійній діяльності. 2. Технології неправдивих повідомлень. Інструменти виявлення неправдивих повідомлень. 3. Види маніпуляцій. Пропаганда як інструментів інформаційного впливу в професійній діяльності. 4.Маніпулювання новинами. Маніпулювання експертними оцінками. Маніпулювання повідомленнями. Маніпуляції з результатами досліджень. **Список рекомендованих джерел:** *Основний: 3 [с. 19, 43-60, 64-79], 4 [с. 97-102].* *Додатковий: 7 [с. 87-90].* *Інтернет-ресурси: 14, 15.*	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)

Тема лекційного заняття	Завдання	Матеріали
1	2	3
ТЕМА 6. *КОМП'ЮТЕРНА ВІРУСОЛОГІЯ* ***Лекція №6*** ***Комп'ютерна вірусологія*** *План лекції №6:* 1. Поняття про комп'ютерні віруси, історія їх виникнення та розвитку. Загальні принципи функціонування комп'ютерних вірусів, їх розмноження. Алгоритми роботи вірусів. 2. Класифікація комп'ютерних вірусів: файлові, завантажувальні (бутові) та файлово-завантажувальні віруси, макровіруси, мережні віруси. 3. Класифікаційний код вірусу. Резидентність, використання стелсалгоритмів, самошифрування та поліморфізм, використання нестандартних методів. 4. Шкідливе програмне забезпечення (ШПЗ). Шляхи розповсюдження ШПЗ, вектори атак. Типи шкідливого програмного забезпечення. Симптоми зараження шкідливим ШПЗ. Шпигунські програми (spyware). 5. Завантажувач (дропер/лоадер). Викрадач інформації «інфостілер або стілер». Keylogger "кейлогер". «JS-сніфери». Троянські програми віддаленого доступу.rat. Банківські трояни (banking trojans). Ransomware (програма-вимагач, програма-шантажист). Майнери (miners). 6. Шкідливе програмне забезпечення для знищення інформації без можливості її відновлення. 7. Рекламне шкідливе програмне забезпечення (adware). **Список рекомендованих джерел:** *Основний: 3 [с. 170-211].* *Додатковий: 7 [с. 69-96].* *Інтернет-ресурси: 14, 15*	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)
ТЕМА 7. *СОЦІАЛЬНА ІНЖЕНЕРІЯ* **Лекція №7** **Соціальна інженерія** *План лекції №7* 1. Поняття соціальної інженерії. Методи соціальної інженерії. 2. Види атак соціальної інженерії. Претекстінг (pretexting). Тейлгейтінг (tailgating). Послуга за послугу (quid pro quo). Злам пароля WI-FI. Атаки грубої сили (brute-force attacks). Прослуховування мережі (network sniffing). 3. Фішингова атака.	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище

Тема лекційного заняття	Завдання	Матеріали
1	2	3
4. Етапи атаки із використанням СІ (соціальної інженерії). Легендування та планування атаки із використання методів СІ. 5. Використання вразливостей як розповсюджений метод проникнення для отримання інформації в професійній діяльності психолога **Список рекомендованих джерел:** *Основний: 2 [с. 112-148], 3 [с. 83-91].* *Додатковий: 6 [с. 136-140], 7 [с. 8-25].* *Інтернет-ресурси: 14.*		Office 365)
ТЕМА 8. СОЦІОТЕХНІЧНА БЕЗПЕКА: ПРОБЛЕМНІ АСПЕКТИ ***Лекція №8*** ***Соціотехнічна безпека: проблемні аспекти*** *План лекції №8* 1. Соціальна інженерія як метод розвідки складних соціальних і соціотехнічних систем в професійній діяльності психолога. 2. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. 3. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки. 4. Соціальні мережі: особливості, основні поняття та визначення. Моніторинг соціальних мереж − цілі та способи реалізації. 5. Поняття соціотехнічної системи та її властивостей. 6. Системний підхід як загальнометодологічний принцип створення складних соціотехнічних систем. **Список рекомендованих джерел:** *Основний: 2 [с. 64-95].* *Додатковий: 6 [с. 144-159], 7 [с. 97-99].* *Інтернет-ресурси: 14*	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)
ТЕМА 9. БЕЗПЕКА СПІЛКУВАННЯ *В* КІБЕРПРОСТО*РІ* **Лекція №9** ***Безпека спілкування в кіберпросторі в професійній діяльності психолога*** *План лекції №9* 1. Захист інформації в глобальних мережах. 2. Характер проведення атак у глобальних мережах. 3. Безпечне користування мережею «Інтернет». 4. Найпоширеніші способи нелегального заробітку в мережі «Інтернет». 5. Безпека браузерів.	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)

Тема лекційного заняття	Завдання	Матеріали
1	2	3
6. Безпека даних в діяльності психолога. 7. Безпечне користування мережами WI-FI. Основні правила безпечного користування WI-FI в діяльності психолога. 8. Безпечне користування месенджерами в професійній діяльності. **Список рекомендованих джерел:** *Основний: 2 [с. 24-43]*. *Додатковий: 6 [с. 495-508], 7 [с. 41-52]*. *Інтернет-ресурси: 14*		
ТЕМА 10. ОСОБЛИВОСТІ ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ В КІБЕРПРОСТОРІ **Лекція №10** ***Особливості економічної діяльності суб'єктів господарювання в кіберпросторі*** *План лекції №10* **1.** Безпека користування соціальними мережами в професійній діяльності психолога. Реєстрація. Стійкий пароль. Оновлення паролів та парольних фраз. **2.** Конфіденційність даних. Налаштування конфіденційності та інших питань безпеки в професійній діяльності психолога. **3.** Безпека мобільних пристроїв. Блокування доступу до пристрою. Безпечна робота в мультимедійних засобах спілкування в професійній діяльності психолога. Передавання вживаних мобільних пристроїв іншим особам. Передавання контактної інформації іншим особам. Вірусне програмне забезпечення. Додаткові функції мобільного пристрою. Головні правила роботи з мобільними пристроями. **4.** Безпека користування електронною поштою в професійній діяльності психолога. Конфіденційність електронної пошти. Найвідоміші атаки через електронну пошту. Загрози під час користування поштовою скринькою. Легітимні та фішингові листи (investigation). **5.** Забезпечення безпеки особистої поштової скриньки (рекомендації). **Список рекомендованих джерел:** *Основний: 2 [с. 130-147], 4[с. 35-49, 68-70]*. *Додатковий: 7 [с. 55-67, 97-99, 105-123]*. *Інтернет-ресурси:*	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)

Тема лекційного заняття	Завдання	Матеріали
1	2	3
ТЕМА 11. БЕЗ ПЕКА ЦИФРОВОГО ПРОСТОРУ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ **Лекція №11** ***Безпека цифрового простору суб'єктів господарювання*** *План лекції №11* **1.** Технічні канали витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів її витоку. **2.** Класифікація каналів витоку інформації. Методи блокування технічних каналів витоку інформації. **3.** Системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації. **4.** Захист акустичної інформації від зняття радіопристроями. **5.** Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами. **6.** Захист інформації від несанкціонованого запису звукозаписувальними пристроями. **7.** Захист електронної інформації в професійній діяльності психолога. **8.** Захист письмової інформації від оптичного зняття в професійній діяльності. **Список рекомендованих джерел:** *Основний: 2 [с. 151-181], 3 [с. 43-60, 290-305].* *Додатковий: 7 [с. 123-127].*	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)
ТЕМА 12. БЕЗПЕКА ІНТЕРНЕТУ-РЕЧЕЙ ***Безпека Інтернету-речей*** *План лекції №12* 1. Історія Інтернету-речей. Екосистема Інтернету-речей. 2. Архітектура Інтернету-речей. Технології Інтернету-речей. «Розумний та безпечний будинок». 3. Анатомія кібератак на IoT-пристрої. Mirai. Stuxnet. Ланцюжкова реакція. Туманні технології. 4. Криптографія. Симетрична криптографія. Асиметрична криптографія. 5. Криптографічний хеш (аутентифікація і цифровий підпис). 6. Інфраструктура відкритого ключа. 7. Блокчейн і криптовалюта в Інтернеті-речей. 8. Рекомендації щодо захисту IoT-пристроїв в професійній діяльності психолога.	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)

Тема лекційного заняття	Завдання	Матеріали
1	2	3
Список рекомендованих джерел: *Основний: 2 [с. 163-167].* *Додатковий: 6 [с. 398-404, 480-482], 9 [с. 15-18, 111-127, 159-170, 189-200].* *Інтернет-ресурси: 14*		
Тема 13. СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПРОНИКНЕННЯ **Лекція №13** ***Системи захисту інформації на проникнення в професійній діяльності психолога*** ***План лекції №13*** **1.** Технології захисту на основі програмного забезпечення. Апаратні засоби захисту. Мережні технології захисту. Хмарні технології захисту в професійній діяльності психолога. **2.** Фізична безпека. Загрози, пов'язані з недотриманням правил фізичної безпеки. Найпопулярніша атака через фізичне втручання: Stuxnet. **3.** Захист інформації за допомогою міжмережних екранів (брандмауера). **4.** Маскування даних. Технології маскування даних. Стеганографія, основні терміни та визначення. Методи та моделі стеганографії. Комп'ютерна і цифрова стеганографія, цифрові водяні позначки. **Список рекомендованих джерел:** *Основний: 1 [с. 188-205], 2 [с. 158-159], 3 [с. 290-312].* *Додатковий: 7 [с. 123-127].* *Інтернет-ресурси: 14*	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)
ТЕМА 14. ОСНОВНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СУБ'ЄКТА ГОСПОДАРЮВАННЯ **Лекція №14** ***Основні методи забезпечення кібербезпеки суб'єкта господарювання*** *План лекції №14* 1. Типи контролю доступу в професійній діяльності психолога. 2. Стратегії контролю доступу. Дискреційне розмежування доступу. Контроль доступу на основі ролей. Розмежування доступу на основі правил. 3. Ідентифікація. Методи аутентифікації. Багатофакторна аутентифікація. Аутентифікація на основі одноразових паролей. Строга аутентифікація.	Передивитись презентацію; ознайомитись із пропонованою додатковою Літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)

Тема лекційного заняття	Завдання	Матеріали
1	2	3
Криптографічні протоколи строгої аутентифікації. Біометрична аутентифікація користувача. Використання авторизації. 4. Типи засобів контролю безпеки. Превентивні засоби контролю. Стримуючі засоби контролю. Коригуючі засоби контролю. Засоби відновлення. Компенсуючі засоби контролю. 5. Криптографія і її основні поняття. Модель криптографічної системи. Принцип Керкхоффса. Етапи розвитку криптографічних систем. Види історичних шифрів. 6. Типи шифрування. Шифрування за допомогою закритого ключа. Процес симетричного шифрування. Типи криптографічних перетворень. Симетричні криптосистеми шифрування. Алгоритм шифрування DES, 3-DES. Стандарт шифрування AES. Основні режими роботи блочного симетричного алгоритму. **Список рекомендованих джерел:** *Основний: 1 [с. 188-193, 205-210], 3 [с. 318-348].* *Додатковий: 6 [с. 398-411, 480-491].* *Інтернет-ресурси: 14*		
Всього – 24 год.		

Схема вивчення дисципліни (лабораторні заняття)

Тема лабораторного заняття	Матеріали та термін виконання
1	4
ТЕМА 1. КІБЕРПРОСТІР І КІБЕРБЕЗПЕКА — ГОЛОВНІ ОЗНАКИ НОВОЇ ІНФОРМАЦІЙНОЇ ЦИВІЛІЗАЦІЇ **Лабораторне заняття №1** **Кібернетичний простір та доступ до системи WWW за допомогою веб-браузера** Мета: 1) поглиблення та закріплення теоретичних знань з наступних питань: - кібернетичний простір: термінологія, структура; - поява та розвиток Інтернет; - основні поняття системи WWW; - структура верхнього рівня веб-браузера. 2) набуття практичних навичок роботи з веб-браузерам **Завдання:** 1) виконати теоретичне завдання згідно з номером варіанту, який приведено в табл. 1, особливо звернути увагу на	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття

Тема лабораторного заняття	Матеріали та термін виконання
1	4
механізми забезпечення інформаційної безпеки в веб-браузера в професійній дяльності психолога. 2) Знайти і обробити інформацію відповідно до завдання та підготувати коротку доповідь (міні-презентацію). 3) провести порівняльний аналіз 2-3 обраних браузерів та сформувати відповідну порівняльну таблицю щодо забезпечення інформаційної безпеки. 4). Оформити звіт згідно до вимог (додаток 1). 5). Зробити висновки, відповісти письмово на контрольні питання та підготуватися до усного опитування.	
ТЕМА 2. НАЦІОНАЛЬНА СИСТЕМА КІБЕРБЕЗПЕКИ УКРАЇНИ **Лабораторне заняття №2** **Інформаційна безпека держави. Потенційні загрози, засоби їх попередження та ліквідації** **Мета:** ознайомитися з поняттям інформаційної безпеки держави та інформаційної війни, основними інтересами України та потенційними небезпеками у сфері інформаційної безпеки, елементами інформаційної боротьби; законодавством України, що стосується інформаційної безпеки держави. **Завдання:** 1) Користуючись однією з пошуковх систем (Google, чи будь-якою іншою) ознайомтеся із законодавчою базою України, що стосується інформаційної безпеки держави. Назви основних законів, указів президента, постанов, положень записати до звіту (не менше 10). 2) На офіційному сайті Верховної ради «Законодавство України» (http://zakon2.rada.gov.ua/laws) знайдіть Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», ознайомтесь з його основними положеннями та занотуйте до звіту такі відомості: - основні стратегічні цілі розвитку інформаційного суспільства в Україні; - основні напрямки розвитку інформаційного суспільства в Україні; - законодавче забезпечення розвитку інформаційного суспільства; - інформаційна безпека в інформаційному суспільстві. 3) Користуючись однією з пошукових систем (Google, чи будь-якою іншою) знайдіть текст Доктрини інформаційної безпеки України, ознайомтесь з основними положеннями та занотуйте до звіту такі відомості: - основні напрями забезпечення державою національного інформаційного суверенітету; - принципи забезпечення інформаційної безпеки України; - основні реальні та потенційні загрози інформаційній безпеці України у сфері державної безпеки; - основні засади державної політики забезпечення інформаційної безпеки України; зробити висновки та письмово дати відповіді на питання.	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття

Тема лабораторного заняття	Матеріали та термін виконання
1	4
ТЕМА 3. СУТНІСТЬ ТА ОСНОВНІ ПРОЦЕДУРИ КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ ***ТЕМА 4. КІБЕРАТАКИ, ЗАГРОЗИ ТА ЇХ ВЛАСТИВОСТІ. ХАРАКТЕРИСТИКА СУЧАСНИХ КІБЕРАТАК*** **Лабораторне заняття №3** **Візуалізація «чорних» хакерів** **Ідентифікація загроз** **Мета:** 1) Вивчення та аналіз інцидентів кібербезпеки. 2) Вивчення можливостей забезпечення функцій безпеки, які використовуються організаціями для збереження даних. З**авдання**: 1) після дослідження та аналізу дати відповіді на запитання: Хто є хакером? До якої організації або групи належить хакер? Який мотив у хакера? Який метод атаки був використаний? Що було метою і в чому була вразливість, використана проти компанії? Як можна було запобігти цій атаці або зменшити її наслідки? 2) Дослідити загрози, що витікають від кібератак. Дослідити тріаду CIA (конфіденційність, цілісність і доступність) та типи кібератак.	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття
ТЕМА 5. ДЕЗІНФОРМАЦІЯ ЯК ЕЛЕМЕНТ КІБЕРАТАК. СЦЕНАРІЇ РОЗВИТКУ ТА МЕТОДИ ПРОТИДІЇ **Лабораторне заняття №4** **Підвищення безпеки облікового запису Google** **Мета:** Захист особистих даних в професійній діяльності. Підвищення безпеки облікового запису Google. Краще зрозуміти заходи безпеки та сервіси, які такі організації, як Google, здійснюють для захисту інформації в професійній діяльності та інформаційних систем . **Завдання:** 1) Проаналізувати можливості функцій безпеки, які використовують такі організації, як Google та Cisco, для захисту даних. Дізнатися як Google гарантує, що сервери, які вони встановлюють у своїх центрах обробки даних (ЦОД), не заражені зловмисним програмним забезпеченням виробниками обладнання. 2) Визначення вразливостей даних. 3) Вміти захистити доступ до облікового запису Gmail.	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін: на лабораторне заняття
ТЕМА 6. КОМП'ЮТЕРНА ВІРУСОЛОГІЯ **Лабораторне заняття №5** **Комп'ютерні віруси: знайомство з принципами роботи. Захист від вірусів в професійній діяльності. Огляд основних антивірусних програм** **Мета:** ознайомитись з основними видами комп'ютерних вірусів, принципами їх роботи поширення і знищення. Розглянути програми для захисту від вірусів, принцип дії, ефективність, можливості. **Завдання:** вибрати один з типів вірусів і описати його за планом: назви вірусів даного типу; принцип роботи даного типу вірусів; методи поширення даного типу вірусів; програми для знищення	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття

Тема лабораторного заняття	Матеріали та термін виконання
1	4
даного типу вірусів; методи для знищення даного типу вірусів. Оформити звіт по роботі та дати письмово відповідь на контрольні питання.	
ТЕМА 7. СОЦІАЛЬНА ІНЖЕНЕРІЯ **Лабораторне заняття №6** **Хто володіє даними: правила надання послуг** **Мета:** Дослідити яким є право власності на особисті дані, якщо вони зберігаються не в локальній системі. Ознайомитися з правилами надання послуг. **Завдання:** дослідити правові угоди, необхідні для використання різних онлайн-сервісів. Дізнатися про деякі способи захисту особистих даних.	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття
ТЕМА 8. СОЦІОТЕХНІЧНА БЕЗПЕКА: ПРОБЛЕМНІ *АСПЕКТИ* ***Лабораторне заняття №7*** ***Інциденти порушення безпеки, несанкціонований доступ до даних*** **Мета:** Знайти інформацію та прочитати про деякі нещодавні порушення безпеки; ознайомитись з декількома інцидентами порушення безпеки, щоб визначити, що було зроблено, які експлойти було використано, і що потрібно зробити, щоб захистити особисті дані в професійній діяльності психолога. **Завдання:** Використовуючи три надані посилання, в яких описано порушення безпеки у різних секторах, заповнити таблицю. Знайти декілька додаткових цікавих випадків порушень кібербезпеки та зазначити їх у висновку в таблиці	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття
ТЕМА 9. БЕЗПЕКА СПІЛКУВАННЯ В КІБЕРПРОСТОРІ **Лабораторне заняття №8** **Захист комп'ютерних мереж та персональних комп'ютерів за допомогою брандмауера (Firewall)** **Мета:** ознайомитися з основним типами, призначенням, базовими функціями брандмауера, зробити загальний огляд вбудованого брандмауера операційної системи Windows. **Завдання:** 1) Виконати послідовність дій Пуск, Панель управления, Система и безопасность, Братмауэр Windows. 2) З'ясувати стан підключення брандмауера. Якщо він відключений – включіть його. Налаштування брандмауера Windows відбувається, в першу чергу, шляхом вказівки "Винятків". 3) Створити виняток для програми, яка повинна приймати вихідні підключення з мережі. Щоб створити виняток потрібно натиснути кнопку "Додати програму ...." відкриється вікно, приклад якого показаний нижче. У цьому вікні в списку програм перераховані ті з них, які встановлені на комп'ютері. Якщо програма, якою необхідно дозволити приймати вхідні підключення, відсутній у списку, то за	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття

Тема лабораторного заняття	Матеріали та термін виконання
1	4
допомогою кнопки Огляд можна вказати шлях до неї. Після натискання кнопки ОК виключення буде створено і додано до списку, де буде зазначено прапорцем, який говорить про те, що дане правило дозволяє зазначеним Додатком відкривати порти і чекати підключення з мережі. Якщо необхідно заборонити додатком відкривати порти, то прапорець слід зняти. 4) Письмово дати відповідь на питання.	
ТЕМА 10. ОСОБЛИВОСТІ ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ В КІБЕРПРОСТОРІ **Лабораторне заняття №9** ***Створення та збереження надійних паролів*** **Мета:** Один із найважливіших способів захистити свої облікові записи в Інтернеті – захистити паролі**.** Зрозуміти концепцію надійного пароля. Необхідно мати різні паролі для різних служб. Часте оновлення паролів є обов'язковим. Рекомендується використання (не дуже розумних або ж навпаки улюблених) фраз як спосіб створення паролів. Потрібно завжди пам'ятати про використання двоетапної перевірки вашого пароля. **Завдання:** Дослідження концепцій створення надійного пароля: створення надійного пароля. Дослідження концепцій безпечного збереження паролів: безпечне зберігання паролів. Використовуючи характеристики надійного пароля, вибрати пароль, який легко запам'ятати, але важко вгадати. Використати для зберігання паролей менеджер паролів.	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття
ТЕМА 11. БЕЗПЕКА ЦИФРОВОГО ПРОСТОРУ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ **Лабораторне заняття №10** ***Перевірка факту компрометації поштової адреси. Двофакторна автентифікація поштового облікового запису*** **Мета:** 1) пересвідчитись у відсутності або наявності витоку власних автентифікаційних даних; 2) відпрацювати навички налаштування двофакторної автентифікації для різних облікових записів. **Завдання:** 1) за адресами https://haveibeenpwned.com , https://monitor.firefox.com перевірити наявність власних поштових облікових записів у «зливах», де фігурують вкрадені дані автентифікації. у випадку знаходження поштових облікових записів у «зливах» терміново змінити паролі на відповідних ресурсах та, за можливості, налаштувати двофакторну автентифікацію; 2) створити безкоштовні особисті поштові облікові записи в доменах gmail.com та protonmail.com. Налаштувати двофакторну автентифікацію через Google Authenticator для облікових записів gmail.com та protonmail.com.	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття

Тема лабораторного заняття	Матеріали та термін виконання
1	4
ТЕМА 12. БЕЗПЕКА ІНТЕРНЕТУ-РЕЧЕЙ **Лабораторне заняття №11** **Використання цифрових підписів** **Мета:** зрозуміти концепції цифрового підпису, оскільки мета цифрового підпису полягає в тому, щоб запобігти підробці та інперсоніфікації цифрових повідомлень **Завдання:** продемонструвати використання цифрових підписів (використовувати веб-сайт для перевірки підпису документа); продемонструвати перевірку цифрового підпису; створення власного цифрового підпису.	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття
ТЕМА 13. СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПРОНИКНЕННЯ **Лабораторне заняття №12** ***Резервне копіювання даних користувача до зовнішнього сховища*** **Мета:** 1) Використання локального зовнішнього диску для резервного копіювання даних; 2) Використання віддаленого диску для резервного копіювання даних. **Завдання:** Дослідити переваги резервного копіювання даних на локальний зовнішній диск. Робота фокусується на Microsoft Backup Utility для виконання резервних копій на локальні зовнішні диски. У другій частині лабораторної роботи використати службу Dropbox для резервного копіювання даних на віддалений або хмарний диск..	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття
ТЕМА 14. ОСНОВНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СУБ'ЄКТА ГОСПОДАРЮВАННЯ **Лабораторне заняття №13** ***Криптографічний вид захисту інформації. Поняття шифрування файлів, папок, повідомлень. Засоби здійснення шифрування інформації в професійній діяльності психолога.*** **Мета:** ознайомитися з поняттям криптографії, способами шифрування файлів, папок, повідомлень та криптографічними методами захисту інформації, розглянути основні засоби здійснення криптографічного захисту інформації; засвоїти принципи, технологію роботи шифрування та дешифрування файлів в професійній діяльності психолога. **Завдання:** 1) Шифр Цезаря — симетричний алгоритм шифрування підстановками. Використовувався римським імператором Юлієм Цезарем для приватного листування. Принцип дії полягає в тому, щоб циклічно зсунути алфавіт, а ключ — це кількість літер, на які робиться зсув. Користуючись алфавітом АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ та використовуючи в якості ключа власний номер в журналі (номер по порядку) зашифрувати повідомлення та записати даний шифр в звіт.	Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365). Термін виконання: на лабораторне заняття

Тема лабораторного заняття	Матеріали та термін виконання
1	4
«Шифр Цезаря має замало ключів — на одиницю менше, ніж літер в абетці. Тому перебрати усі ключі не складає особливої роботи. Дешифрування з одним з ключів дасть нам вірний відкритий текст». 2) Створення і шифрування повідомлення за допомогою інтерактивних методів. У сучасних мережах використовують багато алгоритмів шифрування різних типів. Одним із найбільш безпечних є симетричний алгоритм блокового шифрування (AES). Використовуватимемо засіб, який можна отримати за наступним посиланням: http://aesencryption.net/. Тому будемо використовувати цей алгоритм у роботі для шифрування та дешифрування. 2	

7. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. ISBN 978-617-582-069-8

2. Бурячок В.Л. 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.

3. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.

4. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

Додатковий

5. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.

6. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с. ISBN 978-617-7844-54-8.

7. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікатної) програми підвищення кваліфікації: Практикум. – Київ: ВАІТЕ, 2021. – 106 с.

8. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир: ЖНАЕУ, 2019. – 280 с.

9. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та

технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.

10. Указ Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року "Про Стратегію кібербезпеки України" (дата звернення: 30.06.2022).

11. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України, 2017. – № 45. – Ст.403 (дата звернення: 30.06.2022).

12. Закон України «Про оборону України» // Відомості Верховної Ради України. – 2017. – № 45. – Ст.403 (дата звернення: 30.06.2022).

13. Основи інформаційної безпеки: навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

Інтернет-джерела

14. Cisco -Україна. URL: https://www.cisco.com (дата звернення: 30.06.2022).

15. Annual Threat Reports. URL: https://www.fireeye.com/current-threats/annual-threat-report.html (дата звернення: 30.06.2022).

16. European union agency for cybersecurity. URL: https://www.enisa.europa.eu. (дата звернення: 30.06.2022).

**Курсивом зазначені джерела, що є в наявності в бібліотеці ДТЕУ*

8. Контроль та оцінювання результатів навчання:

Положення про оцінювання результатів навчання студентів і аспірантів наказ КНТЕУ №2891 від 16.09.2019 р. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/NzU4MQ==/69da3a261374f213990591e6e9a812cd.pdf)
Під час вивчення дисципліни викладачем здійснюється поточний та підсумковий контроль. Поточний контроль та оцінювання передбачає:

- перевірку рівня засвоєння теоретичного матеріалу (тестування за матеріалами лекції, який здійснюється з використанням 365 Office);
- захист лабораторних робіт (проходить під час кожної лабораторної роботи);
- перевірка ходу виконання індивідуального завдання (фінальний проєкт);
- перевірка засвоєння матеріалу, що винесений на самостійне опрацювання під час фронтального опитування на лекції та заслуховування доповідей на обрані студентами теми;
- перевірка знань отриманих у ході неформальної освіти (додаткові рекомендовані курси).

Розподіл балів за видами діяльності

Лабораторні роботи, №	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**Сума**
Захист лабораторних робіт (бали)	5	5	5	5	5	5	5	5	5	5	5	5	10	**70**
Практична складова	За проходження курсу «Основи кібезбезпеки» Академії Cisco													**10**
Наукова робота	Участь у всеукраїнських та міжнародних конференціях, олімпіади													**10**
Модульне тестування														**10**
Сума балів														**100**

9. Політика навчальної дисципліни:

Норми етичної поведінки. Всі учасники освітнього процесу, які навчаються в університеті повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку КНТЕУ, загальноприйнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності; підвищувати престиж університету досягненнями в навчанні та науково-дослідницькій діяльності; дбайливо ставитися до університетського майна.

Академічна доброчесність. Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Студенти не видають за свої результати роботи інших людей. При використанні чужих ідей і тверджень у власних роботах обов'язково посилаються на використані джерела інформації. Під час оцінювання результатів навчання не користуються недозволеними засобами, самостійно виконують навчальні завдання, завдання поточного та підсумкового контролю результатів навчання.

Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).

За порушення академічної доброчесності студенти будуть притягнені до академічної відповідальності у відповідності до положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ДТЕУ (Наказ ДТЕУ від 02.02.2018 №377. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/MTEyNDI=/f78c64a74cbbe5b4238729782d707efa.pdf).

Відвідування занять. Відвідування лекційних та лабораторних занять є обов’язковим. Допускаються пропуски занять з таких поважних причин, як

хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).

Правила поведінки під час занять: обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях.

Відпрацювання пропущених занять: У будь-якому випадку студенти зобов'язані дотримуватися термінів виконання усіх видів робіт, передбачених робочою програмою курсу. Відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лабораторне заняття має бути відпрацьоване до наступної пари з використанням ПЗ 365 Office Teams.

Політика електронних пристроїв: Мобільні пристрої дозволяється використовувати на лекціях та під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях.

Політика поведінки в комп'ютерних аудиторіях: Строго забороняється:

- знаходитися в аудиторії у верхньому одязі;
- класти одяг і сумки на столи;
- знаходитися в аудиторії з напоями та їжею;
- працювати на комп`ютері у вологому одязі та вологими руками;
- самостійно намагатися усунути будь-які неполадки в роботі комп'ютера, незалежно від того, коли і з чиєї вини вони сталися;
- класти книги, зошити та інші речі на клавіатуру, монітор і системний блок;
- видаляти і переміщати чужі файли, приносити і запускати комп'ютерні ігри.