КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

СИЛАБУС

ОСНОВИ КІБЕРБЕЗПЕКИ /
CYBERSECURITY ESSENTIALS

SYLLABUS

освітній ступінь	**бакалавр**	/	bachelor
галузь знань	**12 Інформаційні технології**	/	12 Information Technologies
спеціальність	**125 Кібербезпека**	/	125 Cybersecurity

завідувач кафедри О.В. Криворучко

голова методичної ради факультету О.А. Харченко

Київ 2021

Розповсюдження і тиражування без офіційного дозволу КНТЕУ заборонено

Автор: М.В. Сашньова, канд. техн. наук, доцент

Силабус розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки 12 січня 2021р., протокол № 16.

СИЛАБУС

ОСНОВИ КІБЕРБЕЗПЕКИ / CYBERSECURITY ESSENTIALS

SYLLABUS

освітній ступінь	**бакалавр**	/	bachelor
галузь знань	**12 Інформаційні технології**	/	12 Information Technologies
спеціальність	**125 Кібербезпека**	/	125 Cybersecurity

1. **Викладач**:

Лектор: Сашньова Мар'яна Василівна

- *вчене звання та посада*: канд. тех. наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
- *педагогічний стаж* – 10 років;
- *контактиний телефон:* (044)-513-98-62, (044)-531-49-57;
- *e-mail:* m.sashnova@knute.edu.ua
- *наукові інтереси*: новітні інформаційні технології, хмарні технології, технології дистанційного навчання, кібербезпека інформаційних технологій,
- *стажування та підвищення кваліфікації*: **Міжнародне підвищення кваліфікації:**
    - *In the internayional skills development (the webinar) on the theme "THE CLOUD STORAGE SERVICE FOR THE ONLINE STUDYING ON THE EXAMPLE OF THE ZOOM PLATFORM", 10-17th of August, 2020 (Lublin, Republic of Poland).*
    - *In the internayional skills development (the webinar) on the theme "ONLINE LEARNING AS A NON-TRADITIONAL FORM OF THE MODERN EDUCATION ON THE EXEMPLE OF THE MOODLE PLATFORM", 9-16th of November, 2020 (Lublin, Republic of Poland).*
    - *In the internayional skills development (the webinar) on the theme "USING THE OPPORTUNITIES OF CLOUD SERVICES ON THE EXEMPLE OF GOOGLE MEET, GOOGLE CLASSROOM PLATFORM IN THE MODERN ONLINE EDUCATION", 14-21th of Desember, 2020 (Lublin, Republic of Poland).*

  Підвищення кваліфікації в проблемній лабораторії дистанційного навчання Національного технічного університету «Харківський політехнічний інститут» на тему: «Технології розробки дистанційного курсу» (лютий-квітень 2019р.); Інститут науково-дослідний Люблінського науково-технологічного парку та ГО «Міжнародна фундація науковців та освітян».

  Підвищення кваліфікації. *Cisco Networking Academy*. *Сертифікат:* ***Cybersecurity Essentials***, *виданий 27.04.2020;* ***Introduction to Cybersecurity***, *29.06.2020;* ***CCNA Cybersecurity Operations***, *виданий 28.11.2020.*

  Сертифікати: Hack the House – IT Security in a Changing World, 10.06.2020; Академічна доброчесність – запорука успішного розвитку науки і держави, 8 липня 2020 року; Критичне мислення для освітян, 01.07.2020; Можливості хмарних сервісів для організації дистанційного навчання" Початок та практика роботи у MICROSOFT

TEAMS", 20.06.2020; Наукова комунікація в цифрову епоху,11.07.2020; Демонстрація, аналіз і оцінка наукового доробку науковця, 9.07.2020;

2. **Обсяг дисципліни**: **«Основи кібербезпеки»**,
   - рік навчання: I;
   - семестр навчання: 2;
   - кількість кредитів: 6;
   - кількість аудиторних годин на тиждень:
     - лекційних: 2 год.
     - лабораторних: 4 год.

Всього годин / кредитів ЄКТС	Аудиторні заняття, год		Самостійна робота	Вид підсумкового контролю
	Лекції	Лабораторні роботи		
180/6	34	68	78	Іспит

3. **Час та місце проведення:**
   - лекційні заняття - відповідно до розкладу КНТЕУ з врахуванням специфіки дисципліни проведення останньої передбачено 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	середа, 15.10-16.30, on-line
Мова викладання	українська
Інформаційні ресурси за дисципліною	

4. **Пререквізити навчальної дисципліни:**

Дисципліна «Основи кібербезпеки» базується на знаннях, отриманих в результаті вивчення дисципліни «Інформаційні технології у професійній діяльності».

5. **Програмні результати навчання:**

Дисципліна «Основи кібербезпеки», як обов'язкова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем в економіці»: Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інфор-маційних ресурсів і процесів в інформацій-них та інформаційно-телекомунікаційних (автоматизованих) системах; Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інфор-маційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності вико-ристання комплексів засобів захисту в умовах реалізації загроз різних класів; Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; Вирішувати задачі управління процесами відновлення штатного функціонування ін-формаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-

телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки; Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

6. Характеристика дисципліни:

6.1. <u>Мета вивчення дисципліни:</u> *Метою* викладання дисципліни «Основи кібербезпеки» є отримання знань та умінь, які необхідні для успішного виявлення вразливостей у комп'ютерних системах та мережах та усунення проблем безпеки шляхом розробки та впровадження захисних заходів.

6.2. <u>Задачі вивчення дисципліни:</u> Завданням вивчення дисципліни «Основи кібербезпеки» є надання студентам необхідної теоретичної та практичної підготовки для того, щоб вміти:

✓ Використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо безпечного здійснення професійної діяльності;

✓ Аналізувати та виявляти загрози інформації, а також проводити реалізацію алгоритмів шифрування та дешифрування даних;

✓ Аналізувати наслідки кібератак; знати різні категорії вразливостей програмного та апаратного забезпечення і систем безпеки;

✓ Описати принципи конфіденційності, цілісності та доступності відносно стану даних та заходів протидії загрозам в області кібербезпеки;

✓ Прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави, суспільству організації та дестабілізуючі чинники в роботі систем управління;

✓ Описати тактику, методи та процедури, які використовуються кіберзлочинцями;

✓ Описати, як технології, продукти і процедури використовуються для захисту конфіденційності, забезпечення цілісності, забезпечують високу доступність;

✓ Пояснити, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережної інфраструктури.

✓ Розробляти моделі загроз інформації та моделі порушників інформаційної безпеки;

✓ 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.

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

6.4. <u>План вивчення дисципліни:</u>

Схема вивчення дисципліни

Кіл-ть акад. год.	Тема заняття	Форма заняття	Список рекомендо-ваних джерел	Завдання	Матеріали	Вага оцінки (балів)	Термін виконання
30 год.	**РОЗДІЛ 1. ОСНОВНІ ПОЛОЖЕННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ** Кіберпростір і кібербезпека: проблеми, перспективи, технології Загрози у сфері кібербезпеки Розповсюдження загроз кібербезпеки. Дії у кіберпросторі та напрями забезпечення кібербезпеки України	Лекція №1 Лабораторне заняття №1,2 Лекція №2 Лабораторне заняття №3 Лекція №3 Лабораторне заняття №4 Лабораторне заняття №5,6	*Основний: 1, 2, 3.* *Додатковий: 4, 6,7, 9, 10, 11.* *Інтернет-джерела: 13, 14, 15, 16, 17.*	Передивитись презентацію; ознайомитись із пропонованою додатковою літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)	Див. пункт 11, табл.2. «Схема оцінювання за 100-бальною накопичувальною шкалою»	До відповідних лабораторних занять На лабораторне заняття
20 год.	**РОЗДІЛ 2. ТЕХНОЛОГІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ** Сутність та класифікація кібератак на інформаційні системи Технологічні аспекти захисту інформації. Основні процедури керування кібербезпекою	Лекція №4 Лабораторне заняття №7,8 Лекція №5 Лабораторне заняття №9,10	*Основний: 1, 3, 4.* *Додатковий: 5, 6.* *Інтернет-джерела:13, 15.*	Передивитись презентацію; ознайомитись із пропонованою додатковою літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці курсу Microsoft Teams (програмне середовище Office 365)		До відповідних лабораторних занять На лабораторне заняття

20 год.	**РОЗДІЛ 3. КІБЕРБЕЗПЕКА - ЗАГРОЗИ, ВРАЗЛИВОСТІ ТА АТАКИ** Шкідливе програмне забезпечення. Методи і засоби соціального інжинірингу Характеристика сучасних кібератак на інформаційно-комунікаційні технології	Лекція №6 Лабораторне заняття №11,12 Лекція №7 Лабораторне заняття №13,14	*Основний: 1, 3, 4.* *Додатковий: 6.* *Інтернет-джерела:13, 15.*	Передивитись презентацію; ознайомитись із пропонованою додатковою літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці Microsoft Teams (програмне середовище Office 365)		До відповідних лабораторних занять На лабораторне заняття
26 год.	**РОЗДІЛ 4. МИСТЕЦТВО ЗАХИСТУ ТАЄМНИЦЬ** Особливості використання технологій та програмних засобів криптозахисту та криптоаналізу інформації в інформаційних системах Технологічні рішення щодо ідентифікації, автентифікації та авторизації користувачів інформаційної системи. Приховування даних.	Лекція №8 Лабораторне заняття №15 Лабораторне заняття №16,17 Лекція №9 Лабораторне заняття №18 Лабораторне заняття №19,20	*Основний: 1, 2.* *Додатковий: 6.* *Інтернет-джерела:13.*	Передивитись презентацію; ознайомитись із пропонованою додатковою літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці Microsoft Teams (програмне середовище Office 365)		До відповідних лабораторних занять На лабораторне заняття
24 год.	**РОЗДІЛ 5. МИСТЕЦТВО ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ** Типи засобів контролю цілісності даних. Електронний цифровий підпис Принцип розробки баз даних та оформлення запитів за допомогою СУБД Access	Лекція №10 Лабораторне заняття №21,22	*Основний: 1, 2.* *Додатковий: 6.* *Інтернет-джерела:13.*	Передивитись презентацію; ознайомитись із пропонованою додатковою літературою	Презентація, Відеоматеріали		До відповідних лабораторних занять

	Основні відомості про цифрові сертифікати. Забезпечення цілісності баз даних	Лабораторне заняття №23,24 Лекція №11 Лабораторне заняття №25,26		Виконати лабораторну/ самостійну роботу	Завдання на сторінці Microsoft Teams (програмне середовище Office 365)		На лабораторне заняття
16 год.	**РОЗДІЛ 6. КОНЦЕПЦІЯ П'ЯТИ ДЕВ'ЯТОК** Заходи для поліпшення доступності. Технології реагування на інциденти Впровадження заходів аварійного відновлення .	Лекція №12 Лекція №13 Лабораторне заняття №27,28	*Основний: 1, 2, 3. Додатковий: 6. Інтернет-джерела:13, 14.*	Передивитись презентацію; ознайомитись із пропонованою додатковою літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці Microsoft Teams(програмне середовище Office 365)		До відповідних лабораторних занять На лабораторне заняття
20 год.	**РОЗДІЛ 7. ЗАХИСТ ДОМЕНУ КІБЕРБЕЗПЕКИ** Захист систем та пристроїв Укріплення захисту серверів та мережі	Лекція №14 Лабораторне заняття №29,30 Лекція №15 Лабораторне заняття №31,32	*Основний: 1, 2. Додатковий: 6. Інтернет-джерела:13, 14, 15*	Передивитись презентацію; ознайомитись із пропонованою додатковою літературою Виконати лабораторну/ самостійну роботу	Презентація, Відеоматеріали Завдання на сторінці Microsoft Teams(програмне середовище Office 365)		До відповідних лабораторних занять
18 год.	**РОЗДІЛ 8. ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ**		*Основний: 1.*	Передивитись презентацію;	Презентація, Відеоматеріали		До відповідних

	Домени кібербезпеки. Розуміння етики роботи у кібербезпеці, цивільний захист та безпека праці. Організаційний рівень безпеки та підготовки фахівців з кібербезпеки	Лекція №16 Лабораторне заняття №33 Лекція №17 Лабораторне заняття №34	*Додатковий: 6. Інтернет-джерела:13, 16, 17.*	ознайомитись із пропонованою додатковою літературою Виконати лабораторну/ самостійну роботу	Завдання на сторінці Microsoft Teams(програмне середовище Office 365)		лабораторних занять На лабораторне заняття

7. Список рекомендованих джерел

Основний

1. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – О.: ОНАЗ ім. О.С. Попова, 2018. − 228 с. ISBN 978-617-582-064-3

2. Дудатьєв А. В. Захист комп'ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А.- Вінниця ВНТУ, 2010.-219 с.

3. Бурячок В. Л. Інформаційний та кіберпростори : проблеми безпеки, методи та засоби боротьби. Навчальний посібник / В. Л. Бурячок, С.В. Толюпа, В.В. Семко, Л.В. Бурячок, П.М. Складанний, Н.В. Лукова-Чуйко - К. : ДУТ-КНУ, 2016.-178 с.

4. Кавун С. В. Інформаційна безпека : навч. посіб. Ч.1 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків : ХНЕУ, 2008. – 352с. – Бібліогр.: с. 338-349. – ISBN 978-966-676-281-1

Додатковий

5. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І. Вернадського. – К., 2019. – №6 (червень). – 71с.

6. Даник Ю. Г. Основи кібернетичної безпеки: монографія / Ю. Г. Даник, Р. В. Грищук; за заг. ред. проф. Ю. Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.

7. Даник Ю. Г. Визначення сутності та змісту кібернетичної загрози / Ю.Г. Даник, В. І. Шестаков, С. В. Чернишук // Проблеми створення, випробування та експлуатації складних інформаційних систем: зб. наук. праць. – Житомир: ЖВІНАУ, 2012. – Спецвипуск 2. – С. 5-1

8. Присяжнюк М. М. Особливості забезпечення кібербезпеки / М. М. Присяжнюк, Є. І. Цифра // Реєстрація, зберігання та обробка даних. – 2017. – Т. 19. – № 2. –С. 61 – 68.

9. Діордиця І. Кваліфікаційні вимоги до фахівців із кібербезпеки / І. Діордиця // Підприємництво, господарство і право. – 2017. – № 2. – С. 215 – 219. Ю. М. Супрунов // Труди університету. – К. : НУОУ. – 2011. – № 7(106).– С. 5–21.

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".

11. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України, 2017. – № 45. – Ст.403.

12. Закон України «Про оборону України» // Відомості Верховної Ради України. – 2017. – № 45. – Ст.403.

Інтернет-джерела

13. Cisco -Україна. URL: https://www.cisco.com

14. Annual Threat Reports. URL: https://www.fireeye.com/current-threats/annual-threat-report.html

15. European union agency for cybersecurity. URL: https://www.enisa.europa.eu.

16. The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028 (2010). URL:
https://fas.org/irp/doddir/army/pam525-7-8.pdf.

17. U.S. Army War College Strategic Cyberspace Operations Guide (2016). URL:https://info.publicintelligence.net/USArmy-StrategicCO.pdf.

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

8. Контроль та оцінювання результатів навчання:

Положення про оцінювання результатів навчання студентів і аспірантів наказ КНТЕУ №2891 від 16.09.2019р. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/NzU4MQ==/69da3a261374f213990591e6e9a812cd.pdf)

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних, лабораторних занять і оцінюється сумою набраних балів. Обов'язково оцінюються виконана студентами самостійна (індивідуальна) робота, що полягає у розробці дизайну тематичного веб-сайту. Самостійна робота є обов'язковою для кожного студента. Вона вважається виконаною, якщо її оцінено не менше, ніж на 60% від вагового балу.

проміжний/модульний контроль має на меті інтегровану оцінку результатів навчання студента після вивчення матеріалу. Проміжний контроль проходить у вигляді комп’ютерного тестування. Наприкінці семестру проводиться модульна контрольна робота. Модульна контрольна робота також вважається виконаною у разі, якщо її оцінено не менше, ніж на 60% від вагового балу.

підсумковий/семестровий контроль проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу. Підсумковий контроль полягає в оцінюванні рівня засвоєння студентом навчального матеріалу і оволодіння ним необхідними навичками на підставі результатів виконання певних видів робіт на лабораторних заняттях і впродовж виконання самостійного дослідження.

Студент вважається допущеним до семестрового контролю з навчальної дисципліни, якщо він виконав всі види робіт, передбачені робочою програмою. Відповідно до робочої програми навчальної дисципліни бали за кожен вид роботи студента нараховуються наступним чином (див. таблицю 1):

Таблиця 1

Схема оцінювання навчальної дисципліни

Поточний і модульний контроль (100 балів)			**підсумковий/семестровий контроль (100 балів)**	**Сума**
поточний контроль	активність на заняттях	проміжний/модульний контроль	Екзамен	200/2
70 балів	15 балів	15 балів	100 балів	**100**

Підсумкова кількість балів з дисципліни визначається як середнє арифметичне значення отриманих балів за поточний і модульний контроль (враховуючи поточну рейтингову оцінку з навчальних занять, оцінку за виконану самостійну роботу і оцінку за проміжний/модульний контроль) (див. таблицю 2) та складений іспит.

Таблиця 2

Схема оцінювання поточного та модульного контролю

Форми навчання	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	**Сума**
Захист Лабораторних робіт	3		3	3	5		5		5		4		4		3	4		3	4		4		4		4		4		4		4		-		70
Поточні опитування	За проходження курсу «Вступ до кібербезпеки», активність на лекційних заняттях .																																		15
Проміжний/ модульний контроль																5																		10	15
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 КНТЕУ (Наказ КНТЕУ 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.

Підсумковий контроль. Оцінка за курс становить середнє арифметичне значення отриманих балів за поточний і модульний контроль (враховуючи поточну рейтингову оцінку з навчальних занять, оцінку за виконану самостійну роботу і оцінку за проміжний/модульний контроль) та складений іспит, що полягає в оцінюванні рівня засвоєння студентом навчального

матеріалу та набування необхідних навичок на підставі оцінок, отриманих ним на практичних заняттях і за результатами складання екзамену. Перескладання екзамену відбувається у встановлений деканатом термін.

Політика перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності балів).

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