Силабус
освітнього компоненту ОК 12

Інформаційна безпека

Назва дисципліни:	Інформаційна безпека
Рівень вищої освіти:	перший (бакалаврський)
Галузь знань:	G Інженерія, виробництво та будівництво 12 Інформаційні технології
Спеціальність:	G7 Автоматизація, комп'ютерно-інтегровані технології та робототехніка F5 Кібербезпека та захист інформації
Освітньо-професійна:	Кібербезпека автоматизованих, мехатронних і робототехнічних систем
Сторінка курсу в Moodle:	https://dl2022.khadi-kh.com/course/view.php?id=6699
Семестр:	2
Обсяг освітнього компоненту	4 кредита (120 годин)
Форма підсумкового контролю	іспит
Консультації:	за графіком
Назва кафедри:	кібербезпеки
Мова викладання:	українська
Керівник курсу:	Піксасов Михайло Михайлович, к.т.н., доц.
Контактний телефон:	0679449675
E-mail:	mpiks77@gmail.com

Короткий зміст освітнього компоненту:

Мета курсу.

Набуття здобувачами базових теоретичних знань і практичних навичок з основ кібербезпеки та захисту інформації. Формування здатності ідентифікувати, аналізувати та запобігати кіберзагрозам, використовувати сучасні методи та засоби інформаційної безпеки для захисту автоматизованих, мехатронних і робототехнічних систем.

Предмет курсу.

Фундаментальні принципи, поняття та методи кібербезпеки. Вивчаються види кіберзагроз і кіберінцидентів, основи криптографії, методи автентифікації та контролю доступу, принципи побудови систем захисту інформації, правові та організаційні аспекти забезпечення кіберзахисту в сучасних інформаційно-комунікаційних системах.

Передумови для вивчення освітнього компоненту:

Пререквізити:

ОК09 Вступ до фаху.
ОК05 Основи інформаційних технологій.

Постреквізити:

ОК22 Об'єктно-орієнтоване програмування.

Компетентності, яких набуває здобувач:

Інтегральна компетентність. Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації, а також проблеми, що характеризуються комплексністю, під час проєктування та налагодження автоматизованих, мехатронних і робототехнічних систем.

***Загальні компетентності*:**
ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК9. Навички використання інформаційних і комунікаційних технологій.
ЗК10. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел.

Спеціальні (фахові) компетентності:
СК12. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.
СК13. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації в автоматизованих, мехатронних і робототехнічних системах, зокрема у вбудованих пристроях, промислових контролерах, системах керування виробничими процесами та інтелектуальних кіберфізичних комплексах.
СК14. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.
СК16. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).
СК20. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання відповідно до освітньої програми:
РН23. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності, у тому числі для забезпечення стійкості до кіберзагроз у автоматизованих, мехатронних та робототехнічних системах.
РН27. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

Тематичний план

№ теми	Назва тем (ЛК, ПР, СР)	Кількість годин
1	**Лекція 1.** Основні поняття і аналіз загроз інформаційної безпеки.	2
	Лекція 2. Проблеми інформаційної безпеки мереж.	2
	ПР1. Фізична основа кіберпростору – Інтернет. Мережеві утиліти та їх використання для моніторингу та діагностики мережі.	2
	СР1. Основні поняття і аналіз загроз інформаційної та мережевої безпеки. Забезпечення інформаційної безпеки мереж.	4
2	**Лекція 3.** Політики безпеки.	2
	Лекція 4. Стандарти інформаційної безпеки.	2
	ПР2. Аналіз ризиків та основні принципи забезпечення інформаційної безпеки.	2
	СР2. Основні поняття політики безпеки. Структура політики безпеки організації. Роль стандартів інформаційної безпеки.	6
3	**Лекція 5.** Принципи криптографічного захисту інформації.	2
	Лекція 6. Криптографічні алгоритми.	2
	ПР3. Криптографічні методи забезпечення конфіденційності та цілісності інформації.	2
	СР3. Основні поняття криптографічного захисту інформації. Класифікація криптографічних алгоритмів.	4
4	**Лекція 7.** Технології аутентифікації.	2
	Лекція 8. Забезпечення безпеки операційних систем.	2
	ПР4. Інформаційна безпека на рівні операційної системи Windows.	2
	СР4. Аутентифікація, авторизація і адміністрування дій користувачів. Забезпечення безпеки операційних систем.	6
5	**Лекція 9.** Технології міжмережевих екранів.	2
	Лекція 10. Основи технології віртуальних захищених мереж VPN.	2
	ПР5. Інструментальні засоби захисту, firewall.	1
	СР5. Технологій міжмережевих екранів. VPN рішення для побудови захищених мереж.	4
6	**Лекція 11.** Захист на канальному і сеансовому рівнях.	2
	Лекція 12. Захист на мережевому рівні — протокол IPSEC.	2
	ПР6. Дослідження VPN.	1
	СР6. Протоколи формування захищених каналів на канальному і сеансовому рівні. Архітектура засобів безпеки IPSec та особливості реалізації.	6
7	**Лекція 13.** Інфраструктура захисту на прикладному рівні.	2
	Лекція 14. Аналіз захищеності і виявлення атак.	2
	ПР7. Дослідження систем визначення атак (СВА) та типів мережних атак. (Навчально-практичний посібник. Лабораторний практикум з навчальної дисципліни Інформаційна безпека. Кавун С.В.)	2
	СР7. Інфраструктура захисту на прикладному рівні. Технології аналізу захищеності і виявлення атак.	6
8	**Лекція 15.** Захист від вірусів.	2
	Лекція 16. Методи управління засобами мережевої безпеки.	2
	ПР8. Комп'ютерні віруси та інше шкідливе програмне забезпечення. Боротьба з malware.	2

	СР8. Комп'ютерні віруси і проблеми антивірусного захисту. Методи управління засобами мережевої безпеки.	6
Разом	ЛК	32
	ПР	16
	СР	42
	Підготовка до іспиту	30
	Всього	120
	Форма контролю	іспит

Індивідуальне навчально-дослідне завдання (за наявності): **-**

Методи навчання:
МН1- словесний метод (лекція, пояснення, розповідь);
МН2 - практичний метод (практичні заняття);
МН3 - наочний метод (метод ілюстрацій, метод демонстрацій);
МН4 - робота з літературою (навчально-методичною; робота з підручниками і посібниками);

Форми та методи оцінювання
ФМО2 - підсумковий контроль (семестровий іспит);
ФМО3 - усний контроль (бесіда);
ФМО4 - письмовий контроль (індивідуальні завдання);
ФМО5 - тестовий контроль;
ФМО7 - практична перевірка (захист практичних робіт).

Система оцінювання та вимоги:

Поточна успішність

1 Поточна успішність здобувачів за виконання навчальних видів робіт на навчальних заняттях і за виконання завдань самостійної роботи оцінюється за допомогою чотирибальної шкали оцінок з наступним перерахуванням у 100-бальною шкалу. Під час оцінювання поточної успішності враховуються всі види робіт, передбачені навчальною програмою.

1.1 Лекційні заняття оцінюються шляхом визначення якості виконання конкретизованих завдань.

1.2 Практичні заняття оцінюються якістю виконання контрольного або індивідуального завдання, виконання та оформлення практичної роботи.

1.3 Лабораторні заняття оцінюються якістю виконання звітів про виконання лабораторних робіт.

1.4 Семінарські заняття оцінюються якістю виконання індивідуального завдання/реферату.

2 Оцінювання поточної успішності здобувачів вищої освіти здійснюється на кожному практичному занятті (лабораторному чи семінарському) за чотирибальною шкалою («5», «4», «3», «2») і заносяться у журнал обліку академічної успішності.

– «відмінно»: здобувач бездоганно засвоїв теоретичний матеріал, демонструє глибокі знання з відповідної теми або навчальної дисципліни, основні положення;

– «добре»: здобувач добре засвоїв теоретичний матеріал, володіє основними аспектами з першоджерел та рекомендованої літератури, аргументовано викладає його; має практичні навички, висловлює свої міркування з приводу тих чи інших проблем, але припускається певних неточностей і похибок у логіці викладу теоретичного змісту або при аналізі практичного;

– «задовільно»: здобувач в основному опанував теоретичні знання навчальної теми, або дисципліни, орієнтується у першоджерелах та рекомендованій літературі, але непереконливо відповідає, плутає поняття, невпевнено відповідає на додаткові питання, не має стабільних знань; відповідаючи на питання практичного характеру, виявляє неточність у знаннях, не вміє оцінювати факти та явища, пов'язувати їх із майбутньою професією;

– «незадовільно»: здобувач не опанував навчальний матеріал теми (дисципліни), не знає наукових фактів, визначень, майже не орієнтується в першоджерелах та рекомендованій літературі, відсутнє наукове мислення, практичні навички не сформовані.

3 Підсумковий бал за поточну діяльність визнається як середньоарифметична сума балів за кожне заняття, за індивідуальну роботу, поточні контрольні роботи за формулою:

$$K^{поточ} = \frac{K1 + K2 + ... + Kn}{n},$$

де $K^{поточ}$ – підсумкова оцінка успішності за результатами поточного контролю;

$K1, K2, ..., Kn$ – оцінка успішності n-го заходу поточного контролю;

n – кількість заходів поточного контролю.

Оцінки конвертуються у бали згідно шкали перерахунку (таблиця 1).

Таблиця 1 – Перерахунок середньої оцінки за поточну діяльність у багатобальну шкалу

4-бальна шкала	100-бальна шкала	4- бальна шкала	100-бальна шкала	4- бальна шкала	100-бальна шкала	4- бальна шкала	100- бальна шкала
5	100	4,45	89	3,90	78	3,35	67
4,95	99	4,4	88	3,85	77	3,3	66
4,9	98	4,35	87	3,80	76	3,25	65
4,85	97	4,3	86	3,75	75	3,2	64
4,8	96	4,25	85	3,7	74	3,15	63
4,75	95	4,20	84	3,65	73	3,1	62
4,7	94	4,15	83	3,60	72	3,05	61
4,65	93	4,10	82	3,55	71	3	60
4,6	92	4,05	81	3,5	70	від 1,78 до 2,99	від 35 до 59
						повторне складання	
4,55	91	4,00	80	3,45	69	від 0 до 1,77	від 0 до 34
4,5	90	3,95	79	3,4	68	повторне вивчення	

Підсумкове оцінювання

1 Екзамен проводиться після вивчення всіх тем дисципліни і складається здобувачами вищої освіти в період екзаменаційної сесії після закінчення всіх аудиторних занять

2 До екзамену допускаються здобувачі вищої освіти, які виконали всі види робіт передбачені навчальним планом з дисципліни:

- були присутні на всіх аудиторних заняттях (лекції, семінари, практичні);
- своєчасно відпрацювали всі пропущені заняття;

- набрали мінімальну кількість балів за поточну успішність (не менше 36 балів, що відповідає за національною шкалою «3»);

Якщо поточна успішність з дисципліни нижче ніж 36 балів, здобувач вищої освіти має можливість підвищити свій поточний бал до мінімального до початку екзаменаційної сесії.

3 Оцінювання знань здобувачів при складанні екзамену здійснюється за 100-бальною шкалою. Оцінювання знань здобувачів шляхом тестування здійснюється за шкалою:

– «Відмінно»: не менше 90 % правильних відповідей;

– «Дуже добре»: від 82 % до 89 % правильних відповідей;

– «Добре»: від 74 % до 81 % правильних відповідей;

– «Задовільно»: від 67 % до 73% правильних відповідей;

– «Задовільно достатньо»: від 60 % до 66 % правильних відповідей;

– «Незадовільно»: менше 60 % правильних відповідей.

4 Підсумкова оцінка з навчальної дисципліни визначається як середньозважена оцінка, що враховує загальну оцінку за поточну успішність і оцінку за складання екзамену.

5 Розрахунок загальної підсумкової оцінки за вивчення навчальної дисципліни проводиться за формулою:

$$ПК^{екз} = 0,6 \cdot K^{поточ} + 0,4 \cdot E,$$

де $ПК^{екз}$ – підсумкова оцінка успішності з дисциплін, формою підсумкового контролю для яких є екзамен;

$K^{поточ}$ – підсумкова оцінка успішності за результатами поточного контролю (за 100-бальною шкалою);

E - оцінка за результатами складання екзамену (за 100-бальною шкалою).

$0,6$ і $0,4$ – коефіцієнти співвідношення балів за поточну успішність і складання екзамену.

6 За виконання індивідуальної самостійної роботи та участь у наукових заходах здобувачам нараховуються додаткові бали.

6.1 Додаткові бали додаються до суми балів, набраних здобувачем вищої освіти за поточну навчальну діяльність (для дисциплін, підсумковою формою контролю для яких є залік), або до підсумкової оцінки з дисципліни, підсумковою формою контролю для якої є екзамен.

6.2 Кількість додаткових балів, яка нараховується за різні види індивідуальних завдань, залежить від їх об'єму та значимості:

– призові місця з дисципліни на міжнародному / всеукраїнському конкурсі наукових студентських робіт – 20 балів;

– призові місця з дисципліни на всеукраїнських олімпіадах – 20 балів;

– участь у міжнародному / всеукраїнському конкурсі наукових студентських робіт – 15 балів

– участь у міжнародних / всеукраїнських наукових конференціях студентів та молодих вчених – 12 балів;

– участь у всеукраїнських олімпіадах з дисципліни – 10 балів

– участь в олімпіадах і наукових конференціях ХНАДУ з дисципліни – 5 балів;

– виконання індивідуальних науково-дослідних (навчально-дослідних) завдань підвищеної складності – 5 балів.

6.3 Кількість додаткових балів не може перевищувати 20 балів.

7 Загальна підсумкова оцінка за вивчення навчальної дисципліни не може перевищувати 100 балів.

Загальна підсумкова оцінка за вивчення навчальної дисципліни визначається згідно зі шкалою, наведеною в таблиці 2.

Таблиця 2 – Шкала оцінювання знань здобувачів за результатами підсумкового контролю з навчальної дисципліни

Оцінка в балах	Оцінка за національною шкалою		Оцінка за шкалою ЄКТС	
	екзамен	залік	Оцінка	Критерії
90-100	**Відмінно**	**Зараховано**	**A**	Теоретичний зміст курсу освоєний цілком, без прогалин, необхідні практичні навички роботи з освоєним матеріалом сформовані, усі передбачені програмою навчання навчальні завдання виконані, якість їхнього виконання оцінено числом балів, близьким до максимального
80–89	**Добре**	**Зараховано**	**B**	Теоретичний зміст курсу освоєний цілком, без прогалин, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, усі передбачені програмою навчання навчальні завдання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального
75-79			**C**	Теоретичний зміст курсу освоєний цілком, без прогалин, деякі практичні навички роботи з освоєним матеріалом сформовані недостатньо, усі передбачені програмою навчання навчальні завдання виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками
67-74	**Задовільно**		**D**	Теоретичний зміст курсу освоєний частково, але прогалини не носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань, можливо, містять помилки
60–66			**E**	Теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, багато передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального.

Оцінка в балах	Оцінка за національною шкалою		Оцінка за шкалою ЄКТС	
	екзамен	залік	Оцінка	Критерії
35–59	**Незадовільно**	**Не зараховано**	**FX**	Теоретичний зміст курсу освоєний частково, необхідні практичні навички роботи не сформовані, більшість передбачених програм навчання навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання)
0–34	**Неприйнятно**		**F**	Теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, усі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до якого-небудь значущого підвищення якості виконання навчальних завдань (з обов'язковим повторним курсом)

Визнання результатів неформальної та інформальної освіти

Порядок визнання результатів навчання, отриманих у неформальній та інформальній освіті регламентується СТВНЗ-83.1-01:2021 «Визнання результатів неформальної та інформальної освіти».

Для визнання таких результатів належить звернутися із відповідною заявою до декана факультету та додати до неї сертифікати, свідоцтва та інші документи, які підтверджують отримані компетентності. За результатами розгляду заяви створюється предметна комісія, яка розглядає надані документи, проводить співбесіду зі здобувачем і приймає рішення про перезарахування результатів навчання або призначення атестації у вигляді підсумкового контролю (на підготовку дається 10 робочих днів). За результатами контролю комісія виставляє підсумкову оцінку. Якщо здобувач отримав менше 60 балів, то результати навчання у неформальній чи інформальній освіті не зараховуються. При перезарахуванні результатів навчання за дисципліною здобувач звільняється від її вивчення.

Політика курсу:

– курс передбачає роботу в колективі, середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики;

– освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу;

– самостійна робота передбачає вивчення окремих тем навчальної дисципліни, які винесені відповідно до програми на самостійне опрацювання, або ж були розглянуті стисло;

– усі завдання, передбачені програмою, мають бути виконані у встановлений термін;

– якщо здобувач вищої освіти відсутній на заняттях з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача;

– під час вивчення курсу здобувачі вищої освіти повинні дотримуватись правил академічної доброчесності, викладених у таких документах: «Правила академічної доброчесності учасників освітнього процесу ХНАДУ» https://www.khadi.kharkov.ua/fileadmin/P_Standart/pologeniya/stvnz_67_01_dobroch_1.pdf),

«Академічна доброчесність. Перевірка тексту академічних, наукових та кваліфікаційних робіт на плагіат» https://www.khadi.kharkov.ua/fileadmin/P_Standart/pologeniya/stvnz_85.1-02.pdf, «Морально-етичний кодекс учасників освітнього процесу ХНАДУ (https://www.khadi.kharkov.ua/fileadmin/P_Standart/pologeniya/stvnz_67_01_MEK_1.pdf).
– у разі виявлення факту плагіату здобувач отримує за завдання 0 балів і повинен повторно виконати завдання, які передбачені у силабусі;
– списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування.

Рекомендована література:

Основна:

1. Інформаційна безпека. Менеджмент інформаційної безпеки держави [Електронний ресурс]: курс лекцій: навч. посіб. для здобувачів ступеня магістра за освітніми програми Комп'ютерні системи і технології спеціального зв'язку та Спеціальні системи електронних комунікацій спец. 122 Комп'ютерні науки 172 Електронні комунікації та радіотехніка / В. О. Ананьїн, В. В. Горлинський, А. В. Гангал. ІСЗЗІ КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,73 Мбайт). – Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського 2025. – 140 с.
2. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.
3. Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. – Суми : Сумський державний університет, 2021. – 99 с.
4. Навчальний посібник з кібергігієни для закладів вищої освіти зі спеціальними умовами навчання МВС України. Київ, 2024. 230 с.

Додаткова література:

1. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.
2. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах : навч. посіб. — Кропивницький: Видавець Лисенко В. Ф., 2020. — 295 с.
3. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології» / В.П. Полторак; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,73 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 78 с.
4. Дорогий Я.Ю. Методи та засоби технічного захисту інформації. Практикум: електрон. навч. посіб. / Я.Ю. Дорогий, А.О. Нікітенко – Луцьк: ДонНТУ, 2024. – 241 с.
5. Про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. № 994-575. https://zakon.rada.gov.ua/laws/show/994_575#Text
6. Про інформацію : Закон України від 02.10.92 р. № 2657-XII //Відомості Верховної Ради України. – 1992. – № 48. – ст. 650. https://zakon.rada.gov.ua/laws/show/2657-12#Text
7. Закон України «Про захист інформації в інформаційно телекомунікаційних системах» https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

Інтернет-ресурси:

1. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. – 2017. – № 5. – С. 15. – Ст. 102. https://www.president.gov.ua/documents/472017-21374
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Стратегія кібербезпеки України : Указ Президента України від р. № 96/2016// Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899. https://zakon.rada.gov.ua/laws/show/96/2016#Text

4. Системи онлайн-освіти: https://prometheus.org.ua/, https://www.coursera.org, http://www.udacity.com,
5. Портал безпека [Електронний ресурс]. – Режим доступу: https://www.bezpeka.com/uk/golovna/
6. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/
7. Державна служба спеціального зв'язку та захисту інформації: [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua
8. Команда реагування на комп'ютерні надзвичайні події України: [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/

Розробник силабусу навчальної дисципліни
к.т.н., доцент
Михайло ПІКСАСОВ

Гарант освітньої програми
к.т.н., доц. каф. КНІС Сергій НЕРОНОВ

Завідувач кафедри кібербезпеки
к.т.н., доцент Олена КРАЙНЮК