Міністерство освіти і науки України
Сумський національний аграрний університет
Факультет економіки і менеджменту
Кафедра кібернетики та інформатики

Робоча програма (силабус) освітнього компонента

Кібербезпека
(*вибіркова*)

Реалізується в межах освітньої програми **«Інформаційні системи та технології»**

за спеціальністю **126 Інформаційні системи та технології**

на **1 (бакалаврському)** рівні вищої освіти

Суми – 2023

Розробник: _____ Агаджанян-Гонсалес К.Х., ст. викладач кафедри
(підпис)

Розглянуто, схвалено та затверджено на засіданні кафедри кібернетики та інформатики	протокол від 06.06.2023, № 16 Завідувач кафедри _____ Світлана АГАДЖАНОВА (підпис)

Погоджено:

Гарант освітньої програми _____ Світлана АГАДЖАНОВА
(підпис)

Декан факультету,
де реалізується освітня програма _____ Маргарита ЛИШЕНКО
(підпис)

Рецензія на робочу програму(додається) надана: В'юнсенко О.Б. _____

Пасько Н.Б. _____

Методист відділу якості освіти,
ліцензування та акредитації _____ (Баранюк Н.М.)
(підпис) (ПІБ)

Зареєстровано в електронній базі: дата: 14.06 2023 р.

Інформація про перегляд робочої програми (силабусу):

Навчальний рік, в якому вносяться зміни	Номер додатку до робочої програми з описом змін	Зміни розглянуто і схвалено		
		Дата та номер протоколу засідання кафедри	Завідувач кафедри	Гарант освітньої програми

1. ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСВІТНІЙ КОМПОНЕНТ

<table>
<tr><td>1.</td><td>Назва ОК</td><td colspan="8">Кібербезпека</td></tr>
<tr><td>2.</td><td>Факультет/кафедра</td><td colspan="8">Економіки і менеджменту / кібернетики та інформатики</td></tr>
<tr><td>3.</td><td>Статус ОК</td><td colspan="8">варіативна</td></tr>
<tr><td>4.</td><td>Програма/Спеціальність (програми), складовою яких є ОК для (заповнюється для обов’язкових ОК)</td><td colspan="8">Інформаційні системи та технології/126 Інформаційні системи та технології</td></tr>
<tr><td>5.</td><td>ОК може бути запропонований для (заповнюється для вибіркових ОК)</td><td colspan="8"></td></tr>
<tr><td>6.</td><td>Рівень НРК</td><td colspan="8">6-й</td></tr>
<tr><td>7.</td><td>Семестр та тривалість вивчення</td><td colspan="8">8 семестр, 1-15 тижні</td></tr>
<tr><td>8.</td><td>Кількість кредитів ЄКТС</td><td colspan="8">5</td></tr>
<tr><td rowspan="3">9.</td><td rowspan="3">Загальний обсяг годин та їх розподіл</td><td colspan="6">Контактна робота(заняття)</td><td colspan="2">Самостійна робота</td></tr>
<tr><td colspan="2">Лекційні</td><td colspan="2">Практичні /семінарські</td><td colspan="2">Лабораторні</td><td colspan="2"></td></tr>
<tr><td>20</td><td>-</td><td>20</td><td></td><td>-</td><td>-</td><td>110</td><td></td></tr>
<tr><td>10.</td><td>Мова навчання</td><td colspan="8">Українська</td></tr>
<tr><td>11.</td><td>Викладач/Координатор освітнього компонента</td><td colspan="8">старший викладач кафедри кібернетики та інформатики, магістр Агаджанов-Гонсалес Карен Хесусович</td></tr>
<tr><td>11.1</td><td>Контактна інформація</td><td colspan="8">karen.ahadzhanov-honsales@snau.edu.ua; ауд. 308е.</td></tr>
<tr><td>12.</td><td>Загальний опис освітнього компонента</td><td colspan="8">У навчальній дисципліні «Технології захисту інформації» розглядаються теоретичні основи і формуються практичні навички з технологій захисту інформації в автоматизованих інформаційних системах.</td></tr>
<tr><td>13.</td><td>Мета освітнього компонента</td><td colspan="8">Метою курсу є формування базових знань з інформаційних технологій, для можливості орієнтуватися у сучасних напрямках захисту інформації, адміністрування і управління безпекою, аналізу та налагодженню системи безпеки, автоматизації задач налагодження системи безпеки, оцінки безпеки інформаційних технологій, розробки політики інформаційної безпеки та створенню безпечного зовнішнього середовища за стандартом</td></tr>
<tr><td>14.</td><td>Передумови вивчення ОК, зв'язок з іншими освітніми компонентами ОП</td><td colspan="8">1. Освітній компонент базується на ОК Архітектура комп'ютерів, ОК Інформаційні системи та технології.</td></tr>
<tr><td>15.</td><td>Політика академічної доброчесності</td><td colspan="8">При виконання практичних робіт, написанні рефератів та при написання модульних, атестаційних, залікових та екзаменаційних робіт студент обов’язково має дотримуватись правил академічної доброчесності. При виявленні фактів списування або академічної не доброчесності робота виконана студентом анулюється.</td></tr>
<tr><td>16.</td><td>Посилання на курс у системі Moodle</td><td colspan="8">https://cdn.snau.edu.ua/moodle/course/view.php?id=4757</td></tr>
</table>

3. ЗМІСТ ОСВІТНЬОГО КОМОПОНЕНТА (ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ)

Тема. Перелік питань, що будуть розглянуті в межах теми	Розподіл в межах загального бюджету часу								Рекомендована література
	Аудиторна робота						Самостійна робота		
	Лк		П.з / семін. з		Лаб. з.				
	Денна	Заоч.	Денна	Заоч.	Денна	Заоч.	Денна	Заоч.	
Тема 1. *Базові поняття про інформацію та захист інформації* 1.1 Основні поняття інформація. 2.1 Носії інформації. 3.1 Захист інформації	2		2				10		Основна: 1 (с.6-11)
Тема 2. *Структурні компоненти.* 1.1 Фізичні, апаратні, організаційні, програмні, законодавчі та психологічні засоби захисту. 2.1 Керування доступом.	2		2				10		Основна: 1 (с.12-23)
Тема 3. Захист властивостей інформації при передавання в комп'ютерних мережах. 1.1 Захист цілісності з використанням алгоритмів підрахунку контрольних сум Ethernet-пакетів.	2		2				10		Основна: 1 (с.24-28)
Тема 4. *Криптографія* 2.1 Реалізація криптографічних методів захисту (хешування та шифрування) в апаратних засобах ІКС.	2		2				10		Основна: 1 (с.29-33)
Тема 5. *Захист конфіденційності та доступності електронного документу та електронного ресурсу в хмарній системі ЕДО.* 1.1 Налаштування та механізмів доступу до хмарних сховищ електронних документів.	2		2				10		Основна: 1 (с.35-41)
Тема 6. *Система електронного документообігу з точки зору кібербезпеки.* 1.1 Вид та форми електронного документу та властивості ЕД, які підлягають захисту. 2.1 Роль та функції ЕЦП в захисті.	2		2				10		Основна: 1 (с.42-54)

Тема 7. *Шифрування та розшифрування. Типи Raid масивів.*	2		2				10		Основна: 1 (с.55-61)
Тема 8. *Структура системи безпеки ОС Windows, протокол Kerberos.*	2		2				10		Основна: 1 (с.62-73)
Тема 9. *Каталог, Active Directory.*	2		2				10		Основна: 1 (с.83-98)
Тема 10. *Методи і засоби захисту комп'ютерів.* 1.1 Різновиди комп'ютерних вірусів. 2.1 Види шкідливого програмного забезпечення. 3.1 Классификация антивирусных продуктов.	2		2				20		Основна: 1 (с.99-103)
Всього	20	-	20	-	-	-	110	-	

4. МЕТОДИ ВИКЛАДАННЯ ТА НАВЧАННЯ

ДРН	**Методи викладання** (робота, що буде проведена викладачем під час аудиторних занять, консультацій)	**Кіль-кість годин**	**Методи навчання** (які види навчальної діяльності має виконати студент самостійно)	**Кіль-кість годин**
ДРН 1. Здатність застосовувати знання у практичних ситуаціях.	Лекція, практичне заняття, обговорення актуальних питань	10	Опрацювання теоретичного матеріалу, виконання розрахункових завдань	10
ДРН 2. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків	Лекція, практичне заняття, обговорення актуальних питань	10	Опрацювання теоретичного матеріалу, виконання розрахункових завдань	50
ДРН 3. Здатність організовувати збір та зберігання даних у базах та сховищах даних, захист інформації в інформаційних системах та технологіях	Лекція, практичне заняття, обговорення актуальних питань	20	Опрацювання теоретичного матеріалу, виконання розрахункових завдань	50
Всього годин		40		110

5. ОЦІНЮВАННЯ ЗА ОСВІТНІМ КОМПОНЕНТОМ

5.1.Діагностичне оцінювання (зазначається за потреби)

5.2. Сумативне оцінювання

5.2.1. Для оцінювання очікуваних результатів навчання передбачено

№	Методи сумативного оцінювання	Бали / Вага у загальній оцінці	Дата складання (зазначити номер тижня, на якому буде проведено оцінювання)
1.	Практична робота 1-4.	40 балів / 40 %	7 тиждень
2.	Практична робота 5-8.	45 балів / 45 %	14 тиждень
3.	Тестування	15 балів / 15 %	В продовж семестру

5.2.2. Критерії оцінювання

Компонент	**Незадовільно**	**Задовільно**	**Добре**	**Відмінно**
Практична робота 1-4.	*0 балів*	*1-10 балів*	*11-30 балів*	*31-40 балів*
	Завдання не виконано (методика та відповіді неправильні)	*Хід виконання вірний, але наявні суттєві помилки, відповіді, в основному неправильні*	*Завдання виконано, але існують несуттєві помилки*	*Завдання повністю виконано. Помилки відсутні*
Модульний контроль (тест множинного вибору)	0-3 *балів*	4-7 *балів*	*8-10 балів*	*10-15 балів*
	Залежить від кількості вірних відповідей на тест	Залежить від кількості вірних відповідей на тест	Залежить від кількості вірних відповідей на тест	Залежить від кількості вірних відповідей на тест
Практична робота 5-8.	*0 балів*	*1-10 балів*	*11-30 балів*	*31-45 балів*
	Завдання не виконано (методика та відповіді неправильні)	*Хід виконання вірний, але наявні суттєві помилки, відповіді, в основному неправильні*	*Завдання виконано, але існують несуттєві помилки*	*Завдання повністю виконано. Помилки відсутні*

5.3.Формативне оцінювання:

Для оцінювання поточного прогресу у навчанні та розуміння напрямів подальшого удосконалення передбачено

№	**Елементи формативного оцінювання**	**Дата**
1	Усне опитування після вивчення кожної теми	Після завершення вивчення теми
2	Проходження тестування з атестації та модульного контролю зі зворотнім зв’язком з викладачем	Відповідно до графіку навчального процесу

3	Проходження тестування після закінчення вивчення кожної теми для самостійного контролю знань та підготовки до складання заліку (іспиту)	Регулюється студентом самостійно
4	Захист практичних робіт	Через тиждень після їх здачі
5	Усний зворотний зв'язок від викладача під час роботи над практичними роботами протягом занять	На протязі всього семестру

6. НАВЧАЛЬНІ РЕСУРСИ (ЛІТЕРАТУРА)

6.1. Основні джерела

6.1.1. Підручники посібник

1. Тарнавський Ю. А. Технології захисту інформації : підручник для студ. спеціальності 122 «Комп'ютерні науки»; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с. URL: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
2. Проєктування комплексних систем захисту інформації / Ігор Павлов, Володимир Хорошко, Юрій Бабало, Валерій Дудикевич, Іван Опірський, Любомир Пархуць. – Львів : Вид.Львівська політехніка, 2020. – 320с.

6.1.2. Інші джерела

1. Закон України "Про захист персональних даних".
2. Закон України "Про інформацію".
3. Закон України "Про доступ до публічної інформації".
4. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
5. Закон України "Про телекомунікації".
6. Закон України "Про ліцензування видів господарської діяльності".
7. Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 08.10.97 № 1126.
8. Постанова Кабінету Міністрів України від 25.05.2011 № 616 "Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення".
9. Постанова Кабінету Міністрів України від 29.10.00 № 1755 "Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу".
10. Постанова Кабінету Міністрів України від 16.11.2016 № 821 " Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України".
11. Постанова Кабінету Міністрів України від 21.06.17 № 437 "Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності, що підлягає ліцензуванню, у сфері надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України, і встановлюється періодичність проведення планових заходів державного нагляду (контролю) Адміністрацією Державної служби спеціального зв'язку та захисту інформації".

6.3 Програмне забезпечення

1. Система GnuPG https://gnupg.org/
2. Kerberos Protocol Version 5, Release 1.19.2 / 22 July 2021