Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Кафедра безпеки інформації та телекомунікацій

«ЗАТВЕРДЖЕНО»
Завідувач кафедри
_____Корнієнко В.І.
«30» 08 2022р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Системи управління інформаційною безпекою»

Галузь знань ……..…	12 Інформаційні технології
Спеціальність ……...	125Кібербезпека
Освітній рівень…….	другий (магістерський)
Освітньо-професійна програма	Кібербезпека
Спеціалізація ……	-
Статус ……	обов'язкова
Загальний обсяг ..…….	6 кредитів ЄКТС (180 годин)
Форма підсумкового контролю	екзамен
Термін викладання ……..	1-й семестр
Мова викладання …….	українська

Викладач: проф. Корченко А.О.

Пролонговано: на 2024/2025 н.р. _____(Корнієнко В.І.) «02» 09 2024р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

Дніпро
НТУ «ДП»
2022

Робоча програма навчальної дисципліни «Системи управління інформаційною безпекою» для магістрів освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека / Нац. техн. ун-т. «Дніпровська політехніка», каф. безп. інформації та телеком. – Д.: НТУ «ДП», 2022. – 13 с.

Розробники;

Корченко А.О. – д.т.н., професорка, професорка кафедри безпеки інформації та телекомунікацій;

Тимофєєв Д.С. – старший викладач кафедри безпеки інформації та телекомунікацій.

Робоча програма регламентує:

–мету дисципліни;

–дисциплінарні результати навчання, сформовані на основі трансформації очікуваних результатів навчання освітньої програми;

–базові дисципліни;

–обсяг і розподіл за формами організації освітнього процесу та видами навчальних занять;

–програму дисципліни (тематичний план за видами навчальних занять);

–алгоритм оцінювання рівня досягнення дисциплінарних результатів навчання (шкали, засоби, процедури та критерії оцінювання);

–інструменти, обладнання та програмне забезпечення;

–рекомендовані джерела інформації.

Робоча програма призначена для реалізації компетентнісного підходу під час планування освітнього процесу, викладання дисципліни, підготовки студентів до контрольних заходів, контролю провадження освітньої діяльності, внутрішнього та зовнішнього контролю забезпечення якості вищої освіти, акредитації освітніх програм у межах спеціальності.

Погоджено рішенням науково-методичної комісії спеціальності 125 Кібербезпека-(протокол № 1 від 30.08.2022).

ЗМІСТ

1 МЕТА НАВЧАЛЬНОЇ ДИЦИПЛІНИ

В освітньо-професійній програмі Кібербезпека» спеціальності 125 Кібербезпека здійснено розподіл програмних результатів навчання (РН) за організаційними формами освітнього процесу. Зокрема, до дисципліни Ф3 «Системи управління інформаційною безпекою» віднесено такі результати навчання:

РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН14	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

Мета дисципліни– формування у здобувачів вищої освіти компетентностей щодо планування, впровадження, підтримки та модернізації систем управління інформаційною безпекою.

Реалізація мети вимагає трансформації програмних результатів навчання в дисциплінарні та адекватний відбір змісту навчальної дисципліни за цим критерієм.

2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Шифр ПРН	**Дисциплінарні результати навчання (ДРН)**	
	шифр ДРН	**зміст**
РН6	РН6-Ф3	Аналізувати та оцінювати системи управління інформаційною безпекою, комплекси та засобів кіберзахисту, технології використання спеціалізованого програмного забезпечення.
РН7	РН7-Ф3	Розв'язувати складні задачі професійної діяльності в галузі управління інформаційною безпекою на основі обґрунтування використання, впровадження та аналізу кращих світових стандартів,

Шифр ПРН	Дисциплінарні результати навчання (ДРН)	
	шифр ДРН	**зміст**
		практик
РН8	РН8-Ф3	Розробляти і супроводжувати системи управління інформаційної безпеки та кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
РН9	РН9-Ф3	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою організації на базі стратегії і політики інформаційної безпеки.
РН11	РН11-Ф3	Аналізувати та контролювати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки організації.
РН12	РН12-Ф3	Розробляти та впроваджувати методи і заходи протидії кіберінцидентам, надавати рекомендації щодо попередження та аналізу кіберінцидентів.
РН14	РН14-Ф3	Аналізувати, розробляти і супроводжувати заходи аудиту та моніторингу ефективності функціонування інформаційних систем і технологійу сфері інформаційної та\або кібербезпеки.

3 БАЗОВІ ДИСЦИПЛІНИ

Дисципліна викладається у першому семестрі відповідно до навчального плану, тому додаткових вимог до базових дисциплін не встановлюється. Міждисциплінарні зв’язки: вивчення курсу ґрунтується на знаннях, отриманих з вивчених дисциплін за попереднім рівнем освіти.

4 ОБСЯГ І РОЗПОДІЛ ЗА ФОРМАМИ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ТА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Вид навчальних занять	**Обсяг,** *години*	**Розподіл за формами навчання**, *години*			
		денна		**заочна**	
		аудиторні заняття	самостійна робота	аудиторні заняття	самостійна робота
лекційні	115	39	76	8	107
практичні	65	26	39	6	59
лабораторні	-	-	-	-	-
семінари	-	-	-	-	-
РАЗОМ	180	65	115	14	166

5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Шифри ДРН	**Види та тематика навчальних занять**	**Обсяг складових,** *години*
	ЛЕКЦІЇ	**115**
РН6-Ф3	**1 Характеристика та обрання основних підходів до управління інформаційною безпекою**	20

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, *години*
	1. Базова термінологія 1.1. Система 1.2. Системний підхід 1.3. Процес 1.4. Процесний підхід 1.5. Управління 1.6. Циклічна модель поліпшення процесів 1.7. Системний підхід до управління організацією 1.8. Процесний підхід до управління організацією 1.9. Інформаційна безпека	
РН7-Ф3, РН12-Ф3, РН14-Ф3,	**2 Аналіз та застосування основних стандартів з систем і процесів управління інформаційною безпекою**	40
	2. Стандартизація систем і процесів управління інформаційною безпекою 2.1. Серія стандартів ISO / IEC 27000 «Інформаційні технології. Методи забезпечення безпеки » 2.1.1. ISO / IEC 27000- СУІБ: визначення та основні принципи 2.1.2. ISO / IEC 27001 вимоги до СУІБ 2.1.3. ISO / IEC 27002 практичні правила управління ІБ 2.1.4. ISO / IEC 27003 посібник з впровадження СУІБ 2.1.5. ISO / IEC 27004 оцінка функціонування СУІБ 2.1.6. ISO / IEC 27005 управління ризиками ІБ 2.1.9. ISO / IEC 27011 посібник з управління ІБ для телекомунікаційних компаній на основі ISO / IEC 27002 2.1.10. ISO / IEC 27013 - керівництво з інтегрованого впровадження стандартів ISO / IEC 20000 і 27001 2.1.11. ISO / IEC 27014 - інфраструктура керівництва ІБ 2.1.12. ISO / IEC 27015 - керівництво з управління ІБ для фінансових сервісів 2.1.13. ISO / IEC 27031 - керівництво по готовності інформаційних і телекомунікаційних технологій для забезпечення безперервності бізнесу 2.1.14. ISO / IEC 27033 - управління безпекою мереж 2.1.15. ISO / IEC 27035-управління інцидентами ІБ 2.1.16. ISO / IEC 27037- керівництво по ідентифікації, збору та / або отриманню і забезпеченню збереження свідчень, представлених в електронній формі 2.2. Стандарти на окремі процеси управління ІБ і оцінку безпеки ІТ 2.2.1. ISO / IEC 13335 - методи і засоби забезпечення безпеки інформаційних технологій 2.2.2. ISO / IEC 15408 та ISO / IEC 18045 - загальні критерії та методології оцінки безпеки інформаційних технологій	
РН9-Ф3, РН11-Ф3	**3 Розробка та аналіз політики інформаційної безпеки** 3. Політика інформаційної безпеки 3.1. Поняття політики забезпечення ІБ і політики ІБ організації 3.2. Причини розробки політики ІБ 3.3. Основні вимоги та принципи, що враховуються при розробці та впровадженні політики ІБ	30

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, *години*
	3.4. Зміст політики ІБ 3.4.1. Зміст корпоративної політики ІБ 3.4.2. Зміст приватних політик ІБ 3.5. Життєвий цикл політики ІБ 3.5.1. Розробка політики ІБ 3.5.2. Впровадження політики ІБ 3.5.3. Застосування політики ІБ 3.5.4. Анулювання політики ІБ 3.6. Відповідальність за виконання політики ІБ	
РН8-Ф3	**4 Запровадження управління ІБ із застосуванням СУІБ**	25
	4. Управління і система управління інформаційною безпекою 4.1. Необхідність управління забезпеченням ІБ організації 4.2. Діяльність по забезпеченню ІБ організації як процес 4.3. Визначення управління ІБ організації 4.4. Управління ІБ інформаційно-телекомунікаційних технологій організації 4.5. Система управління ІБ організації 4.5.1. Область дії СУІБ 4.5.2. Документальне забезпечення СУІБ 4.5.3. Політика СУІБ 4.5.4. Підтримка СУІБ з боку керівництва	
	ПРАКТИЧНІ ЗАНЯТТЯ	**65**
РН6-Ф3, РН7-Ф3, РН8-Ф3, РН9-Ф3, РН11-Ф3 РН12-Ф3, РН14-Ф3,	Дослідження реальних об’єктів інформаційної діяльності	10
	Розробка проекту реалізації СУІБ	10
	Інвентаризація та класифікація інформаційних активів	15
	Програмне моделювання процесу управління ризиками інформаційної безпеки	15
	Розробка політики безпеки інформації	15
	РАЗОМ	**180**

6 ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Сертифікація досягнень студентів здійснюється за допомогою прозорих процедур, що ґрунтуються на об’єктивних критеріях відповідно до «Положення про оцінювання результатів навчання здобувачів вищої освіти».

Досягнутий рівень компетентностей відносно очікуваних, що ідентифікований під час контрольних заходів, відображає реальний результат навчання студента за дисципліною.

6.1 Шкали

Оцінювання навчальних досягнень студентів НТУ «ДП» здійснюється за рейтинговою (100-бальною) та інституційною шкалами. Остання необхідна (за

офіційною відсутністю національної шкали) для конвертації (переведення) оцінок мобільних студентів.

Шкали оцінювання навчальних досягнень студентів НТУ «ДП»

Рейтингова	Інституційна
90…100	відмінно / Excellent
74…89	добре / Good
60…73	задовільно / Satisfactory
0…59	незадовільно / Fail

Кредити навчальної дисципліни зараховуються, якщо студент отримав підсумкову оцінку не менше 60-ти балів. Нижча оцінка вважається академічною заборгованістю, що підлягає ліквідації.

6.2 Засоби та процедури

Зміст засобів діагностики спрямовано на контроль рівня сформованості знань, умінь/навичок, комунікації, автономії та відповідальності студента за вимогами НРК до 7-го кваліфікаційного рівня під час демонстрації регламентованих робочою програмою результатів навчання.

Засоби діагностики (контрольні завдання) для поточного та підсумкового контролю дисципліни затверджуються кафедрою.

Види засобів діагностики та процедур оцінювання для поточного та підсумкового контролю дисципліни подано нижче.

Засоби діагностики та процедури оцінювання

ПОТОЧНИЙ КОНТРОЛЬ			**ПІДСУМКОВИЙ КОНТРОЛЬ**	
навчальне заняття	**засоби діагностики**	**процедури**	**засоби діагностики**	**процедури**
лекції	контрольні завдання за кожною темою	виконання завдання під час лекцій	Комплексна контрольна робота (ККР)	визначення середньозваженого результату поточних контролів; виконання ККР під час екзамену за бажанням студента
практичні	контрольні завдання за кожною темою	виконання завдань під час практичних занять		
	та індивідуальне завдання	виконання завдань під час самостійної роботи		

Під час поточного контролю лекційні заняття оцінюються шляхом визначення якості виконання контрольних конкретизованих завдань. Практичні заняття оцінюються якістю виконання контрольного та індивідуального завдання.

За наявності рівня результатів поточних контролів з усіх видів навчальних занять не менше 60 балів, підсумковий контроль здійснюється без участі студента шляхом визначення середньозваженого значення поточних оцінок.

Незалежно від результатів поточного контролю кожен студент під час екзамену має право виконувати ККР, яка містить завдання, що охоплюють ключові дисциплінарні результати навчання.

Кількість конкретизованих завдань ККР повинна відповідати відведеному часу на виконання. Кількість варіантів ККР має забезпечити індивідуалізацію завдання.

Значення оцінки за виконання ККР визначається середньою оцінкою складових (конкретизованих завдань) і є остаточним.

3 Критерії

Для оцінювання виконання контрольних завдань під час поточного контролю лекційних і практичних занять в якості критерія використовується коефіцієнт засвоєння, що автоматично адаптує показник оцінки до рейтингової шкали:

$$O_i = 100\ a/m,$$

де a – число правильних відповідей або виконаних суттєвих операцій відповідно до еталону рішення; m – загальна кількість запитань або суттєвих операцій еталону.

Індивідуальні завдання та комплексні контрольні роботи оцінюються експертно за допомогою критеріїв, що характеризують співвідношення вимог до рівня компетентностей і показників оцінки за рейтинговою шкалою.

Зміст критеріїв спирається на компетентністні характеристики, визначені НРК для магістерського рівня вищої освіти (подано нижче).

Загальні критерії досягнення результатів навчання для 7-го кваліфікаційного рівня за НРК

Опис кваліфікаційного рівня	**Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії**	**Показник оцінки**
	Знання	
– спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та	Відповідь відмінна – правильна, обґрунтована, осмислена. Характеризує наявність: – спеціалізованих концептуальних знань на рівні новітніх досягнень; – критичне осмислення проблем у навчанні та/або професійній діяльності та на межі предметних галузей	95-100
	Відповідь містить не грубі помилки або описки	90-94
	Відповідь правильна, але має певні неточності	85-89
	Відповідь правильна, але має певні неточності й недостатньо обґрунтована	80-84
	Відповідь правильна, але має певні неточності, недостатньо обґрунтована та осмислена	74-79
	Відповідь фрагментарна	70-73
	Відповідь демонструє нечіткі уявлення студента про	65-69

Опис кваліфікаційного рівня	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показник оцінки
на межі галузей знань	об’єкт вивчення	
	Рівень знань мінімально задовільний	60-64
	Рівень знань незадовільний	<60
Уміння/навички		
– спеціалізовані уміння/навички розв’язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур; – здатність інтегрувати знання та розв’язувати складні задачі у широких або мультидисципліна рних контекстах; – здатність розв’язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	Відповідь характеризує уміння: – виявляти проблеми; – формулювати гіпотези; – розв’язувати проблеми; – оновлювати знання; – інтегрувати знання; – провадити інноваційну діяльність; – провадити наукову діяльність	95-100
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності з не грубими помилками	90-94
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації однієї вимоги	85-89
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації двох вимог	80-84
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації трьох вимог	74-79
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації чотирьох вимог	70-73
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності при виконанні завдань за зразком	65-69
	Відповідь характеризує уміння/навички застосовувати знання при виконанні завдань за зразком, але з неточностями	60-64
	Рівень умінь/навичок незадовільний	<60
Комунікація		
– зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	Зрозумілість відповіді (доповіді). *Мова:* – правильна; – чиста; – ясна; – точна; – логічна; – виразна; – лаконічна. *Комунікаційна стратегія:* – послідовний і несуперечливий розвиток думки; – наявність логічних власних суджень; – доречна аргументації та її відповідність	95-100

Опис кваліфікаційного рівня	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показник оцінки
	відстоюваним положенням; – правильна структура відповіді (доповіді); – правильність відповідей на запитання; – доречна техніка відповідей на запитання; – здатність робити висновки та формулювати пропозиції; – використання іноземних мов у професійній діяльності	
	Достатня зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія з незначними хибами	90-94
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано три вимоги)	85-89
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано чотири вимоги)	80-84
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано п’ять вимог)	74-79
	Задовільна зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано сім вимог)	70-73
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано дев’ять вимог)	65-69
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано 10 вимог)	60-64
	Рівень комунікації незадовільний	<60
Відповідальність і автономія		
– управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів; – відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів; – здатність	Відмінне володіння компетенціями: – використання принципів та методів організації діяльності команди; – ефективний розподіл повноважень в структурі команди; – підтримка врівноважених стосунків з членами команди (відповідальність за взаємовідносини); – стресовитривалість; – саморегуляція; – трудова активність в екстремальних ситуаціях; – високий рівень особистого ставлення до справи; – володіння всіма видами навчальної діяльності; – належний рівень фундаментальних знань; – належний рівень сформованості загальнонавчальних умінь і навичок	95-100
	Упевнене володіння компетенціями відповідальності і автономії з незначними хибами	90-94
	Добре володіння компетенціями відповідальності і	85-89

Опис кваліфікаційного рівня	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показник оцінки
продовжувати навчання з високим ступенем автономії	автономії (не реалізовано дві вимоги)	
	Добре володіння компетенціями відповідальності і автономії (не реалізовано три вимоги)	80-84
	Добре володіння компетенціями відповідальності і автономії (не реалізовано чотири вимоги)	74-79
	Задовільне володіння компетенціями відповідальності і автономії (не реалізовано п’ять вимог)	70-73
	Задовільне володіння компетенціями відповідальності і автономії (не реалізовано шість вимог)	65-69
	Задовільне володіння компетенціями відповідальності і автономії (рівень фрагментарний)	60-64
	Рівень відповідальності і автономії незадовільний	<60

7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Технічні засоби навчання: мультимедійні та комп’ютерні пристрої.

Програмні засоби дистанційної освіти: MS Office 365, MS Teams, дистанційна платформа Moodle.

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1.Шелест, М.Є., Корченко, О.Г., Іванченко, Є.В., Ткач, Ю.М. , Казмірчук, С.В. Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125" Кібербезпека".Ніжин : ФОП Лук’яненко В.В. ТПК «Орхідея», 2019. – 408 с.

2. Закон України Про захист інформації в інформаційно-телекомунікаційних системах № 80/94-ВР від 05.07.1994 р., [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

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

4. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

5. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

6. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

7. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT)

Навчальне видання

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Системи управління інформаційною безпекою» для магістрів спеціальності 125-Кібербезпека

Розробники:
КорченкоАнна Олександрівна
Тимофєєв Дмитро Сергійович