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
«Технології забезпечення інформаційної і кібербезпеки об'єктів»

Галузь знань ……..…	12 Інформаційні технології
Спеціальність ……...	125 Кібербезпека
Освітній рівень…….	Другий(магістерський)
Освітньо-професійна програма	Кібербезпека
Спеціалізація ……	
Статус ……	обов'язкова
Загальний обсяг ..…….	8 кредитів ЄКТС (240 годин)
Форма підсумкового контролю	іспит
Термін викладання ……..	1-й семестр
Мова викладання …….	українська

Викладач: доц. Ковальова Ю.В.

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

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

Дніпро
НТУ «ДП»
2022

Робоча програма навчальної дисципліни «Технології забезпечення інформаційної і кібербезпеки об’єктів» для магістрів спеціальності 125 «Кібербезпека» / Нац. техн. ун-т. «Дніпровська політехніка», каф. безп. інф. та телеком. – Д.: НТУ «ДП», 2022. – 12 с.

Розробник – Ковальова Ю.В., к.т.н., доцент 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 Національного технічного університету «Дніпровська політехніка» спеціальності 125 «Кібербезпека» здійснено розподіл програмних результатів навчання (РН) за організаційними формами освітнього процесу. Зокрема, до дисципліни Ф1 «Технології забезпечення інформаційної і кібербезпеки об'єктів» віднесено такі результати навчання:

РН3	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН13	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

Мета дисципліни – формування у студентів компетентностей щодо принципів впровадження технології забезпечення інформаційної і кібербезпеки об'єктів.

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**
РН3	РН3-Ф1	Використовувати сучасні технології забезпечення інформаційної і кібербезпеки об'єктів при реалізації дослідницької діяльності в сфері інформаційної безпеки та/або кібербезпеки.

РН4	РН4-Ф1	Застосовувати, розробляти та удосконалювати інформаційні технології, математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки на основі сучасних технологій забезпечення інформаційної і кібербезпеки об'єктів.
РН5	РН5-Ф1	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема із використанням сучасних технологій забезпечення інформаційної і кібербезпеки об'єктів.
РН6	РН6-Ф1	Аналізувати та оцінювати захищеність систем та засобів кіберзахисту, технології створення та використання сучасних технологій забезпечення інформаційної і кібербезпеки об'єктів.
РН10	РН10-Ф1	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН13	РН13-Ф1	Розробляти та використовувати сучасні технології забезпечення інформаційної і кібербезпеки об'єктів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

3 БАЗОВІ ДИСЦИПЛІНИ

Базовими дисциплінами є дисципліни які вивчалися студентами на освітньому рівні бакалавр, що формують компетентності щодо здатності застосовувати теоретичні та практичні основи вищої математики, програмування та інформаційних технологій в процесі розв'язування прикладних задач.

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	150	39	111	8	142
практичні	90	26	64	8	82
лабораторні	-				
семінари	-				
РАЗОМ	240	65	175	16	224

5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Шифри ДРН	**Види та тематика навчальних занять**	**Обсяг складових,** *години*
	ЛЕКЦІЇ	**150**
РН3-Ф1	**Технології забезпечення інформаційної безпеки.**	**90**

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, *години*
РН4-Ф1 РН5-Ф1 РН6-Ф1 РН10-Ф1 РН13-Ф1	1. Основні принципи забезпечення національної безпеки	8
	2. Загрози кібербезпеці і безпеці інформаційних ресурсів	8
	3. Національні інтереси держави в інформаційній сфері.	8
	4. Основні напрями державної політики з питань національної безпеки в інформаційній сфері	8
	5. Кібершпіонаж як частина побудови системи безпеки	8
	6. Технічні канали витоку інформації.	8
	7. Способи несанкціонованого зняття інформації з технічних каналів її витоку	8
	8. Стратегічні комунікації як вектор розвитку інформаційної безпеки	8
	9. Основні фактори впливу методів проведення кібероперацій	8
	10. Концепція суспільних зв'язків як системи впливу на людей у секторі безпеки	8
	11. Заходи щодо боротьби з кіберзлочинністю	10
РН3-Ф1 РН4-Ф1 РН5-Ф1 РН6-Ф1 РН10-Ф1 РН13-Ф1	**Кіберзахист об’єктів критичної інфраструктури**	**60**
	12. Вплив зовнішніх атак на об’єкти стратегичного значення	14
	13. Методика та вплив ведення інформаційних війн на державному рівні	16
	14. Інформаційне забезпечення зв'язків з громадськістю в секторі безпеки	10
	15. Сучасні технології захисту інформації об’єктів критичної інфраструктури	20
	ПРАКТИЧНІ ЗАНЯТТЯ	**90**
РН3-Ф1 РН4-Ф1 РН5-Ф1 РН6-Ф1 РН10-Ф1 РН13-Ф1	1. Світовий досвід побудови системи інформаційної безпеки на об’єктах стратегічного значення	14
	2. Побудова принципів впровадження нормативних актів в систему інформаційного захисту	16
	3. Класифікація каналів витоку інформації	14
	4. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів її витоку	14
	5. Методи та засоби блокування технічних каналів витоку інформації	16
	6. Методи захисту інформації у телекомунікаційних мережах та відкритих каналах зв’язку	16
		240

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 компетентності 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 зараховується, 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

<table>
<tr><th colspan="3">ПОТОЧНИЙ КОНТРОЛЬ</th><th colspan="2">ПІДСУМКОВИЙ КОНТРОЛЬ</th></tr>
<tr><th>навчальне заняття</th><th>засоби діагностики</th><th>процедури</th><th>засоби діагностики</th><th>процедури</th></tr>
<tr><td>лекції</td><td>контрольні завдання за кожною темою</td><td>виконання завдання під час лекцій</td><td rowspan="2">комплексна контрольна робота (ККР)</td><td rowspan="2">визначення середньозваженого результату поточних контролів;
виконання ККР під час екзамену за бажанням студента</td></tr>
<tr><td>практичні</td><td>контрольні завдання за кожною темою</td><td>виконання завдань під час практичних занять</td></tr>
</table>

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

6.3 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 компетентнісні характеристики, визначені НРК для магістерського рівня вищої освіти.

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 на межі галузей знань	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 об’єкт вивчення	65-69
	Рівень знань мінімально задовільний	60-64

Опис кваліфікаційного рівня	**Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії**	**Показник оцінки**
	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 відстоюваним положенням; – правильна структура відповіді (доповіді); – правильність відповідей на запитання;	95-100

Опис кваліфікаційного рівня	**Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії**	**Показник оцінки**
	– 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 продовжувати навчання з високим ступенем автономії	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 автономії (не реалізовано дві вимоги)	85-89
	Добре володіння компетенціями відповідальності і автономії (не реалізовано три вимоги)	80-84
	Добре володіння компетенціями відповідальності і	74-79

Опис кваліфікаційного рівня	**Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії**	**Показник оцінки**
	автономії (не реалізовано чотири вимоги)	
	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. Ковальова Ю.В. Технологічні аспекти побудови мереж інформаційної безпеки об’єктів критичної інфраструктури. Монографія «Innovative Technologies in the Formation and Development of Human Capital», Вища Технічна Школа, м. Катовіца, Польша, 2018. С. 27-37.ISBN: 978–83–947093–6–5.
2. Рибальський О.В., Смаглюк В.М., Хахановський В.Г. Основи інформаційної безпеки, підручник для курсантів ВНЗ МВС України, 2011.
3. Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. — К.: ІСЗЗІ КПІ ім. Ігоря Сікорського», 2018. — 297 с.
4. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. – К.: Видавництво НА СБ України, 2020. – 256 с.
5. YuliiaKovaleva, TetianaBabenko, ViraIgnisca. Models And Methods Of Wireless Decentralized Networks For Energy Monitoring Of Critical Infrastructure Facilities. Scientific and practica lcybersecurity journal. Georgia. Issue No: 4, December, 2020. ISSN 2587-4667 https://journal.scsa.ge/issue/december-2020/
6. Zhang Z., Mehmood A., Shu L., Huo Z., Zhang Y., Mukherjee M. A survey on fault diagnosis in wireless sensor networks. IEEE Access, vol. 6, pp. 11349-11364, 2018.
7. Kovalova Y., Babenko T., Oksiiuk O., Myrutenko L. Optimization of Lifetime In Wireless Monitoring Networks. Internationa lJournal of Computing. Research Institute for Intelligent Computer Systems, 2020 № 19 (2), Pp. 267–272. ISSN: 2312-5381.
8. KathrynCave. TheIoT “timebomb” report: 49 security experts share their views.- http://www.idgconnect.com/abstract/12744/the-iot-bomb-report-49-security-experts-share-views
9. Nelles O. Nonlinear System Identification: From Classical Approaches to Neural and Fuzzy Models / O. Nelles. – Berlin: Springer, 2001. – 785 pp.
10. Дистанційна платформа: **https://do.nmu.org.ua/course/view.php?id=5375**

Навчальне видання

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Технології забезпечення інформаційної і кібербезпеки об’єктів» для магістрів спеціальності 125 «Кібербезпека»

Розробник:
Ковальова Юлія Вікторівна