

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

Кафедра безпеки інформації та телекомунікацій



«ЗАТВЕРДЖЕНО»

Завідувач кафедри
Корнієнко В.І.
«20» 05 2022р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Програмні методи захисту інформації»

Галузь знань	12 Інформаційні технології
Освітній рівень.....	Другий (магістерський)
Статус.....	вибіркова
Загальний обсяг	4кредитів ЄCTS (120 годин)
Форма підсумкового контролю	диференційований залік
Термін викладання	2-й семестр
Мова викладання	українська

Викладач: доц. Сафаров О.О.

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 «Програмні методи захисту інформації» для магістрів галузі знань 12 Інформаційні технології / Нац. техн. ун-т. «Дніпровська політехніка», каф. безпеки інформації та телекомунікацій – Д. : НТУ «ДП», 2022. – 12 с.

Розробник:

Сафаров О.О., 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.

ЗМІСТ

1 МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ	4
2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ.....	4
3 БАЗОВІ ДИСЦИПЛІНИ.....	4
4 ОБСЯГ І РОЗПОДІЛ ЗА ФОРМАМИ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ТА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ	4
5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ.....	4
6 ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ.....	5
6.1 Шкали.....	5
6.2 Засоби та процедури	5
6.3 Критерії.....	7
7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ	12
8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ.....	12

1 МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета дисципліни – закласти термінологічний фундамент, навчити здобувачів правильно проводити аналіз загроз інформаційній безпеці, основним методам, принципам, алгоритмам та засобам захисту інформації в комп'ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів та засобів здійснення погроз зі сторони потенційних порушників.

2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Дисциплінарні результати навчання (ДРН)		
шифр ДРН	зміст	
ВР1	Використовувати технології розроблення програмних засобів захисту інформації, синтезу комплексів засобів захисту інформації.	
ВР2	Застосувувати математичне та комп'ютерне моделювання для вирішення широкого спектру задач синтезу комплексів засобів захисту інформації.	

3 БАЗОВІ ДИСЦИПЛІНИ

Дисципліна «Програмні методи захисту інформації» викладається в 2-му семестрі відповідно до навчального плану. Додаткових вимог до базових дисциплін не встановлюється.

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	80	38	42	6	74
практичні	40	19	21	4	36
РАЗОМ	120	57	63	10	110

5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
	ЛЕКЦІЇ	80
ВР1	Тема 1. Базові поняття інформаційної безпеки Основні поняття. Захист інформації та його основні завдання. Класифікація загроз для інформації та їх джерел. Поняття про інформацію з обмеженим доступом. Структура політики безпеки та її основні частини.	8

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
ВР1	Тема 2. Механізми і політики розмежування прав доступу TCSEC - перший стандарту галузі оцінки захищеності комп'ютерних систем. Common Criteria - європейський стандарт у галузі оцінки захищеності комп'ютерних систем. Вимоги довіри. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу"	8
ВР1	Тема 3. Шифрування даних. Основні поняття роботи К. Шеннона "Теорія зв'язку в секретних системах". Симетричні, асиметричні та комбіновані криптосистеми. Їх переваги та недоліки.	8
ВР1	Тема 4. Системи захисту програмного забезпечення. Мета і доцільність використання систем захисту. Класифікація системи захисту інформації. Пакувальники/шифратори. Системи захисту від несанкціонованого копіювання. Системи захисту від несанкціонованого доступу. Основні алгоритми захисту програмного забезпечення.	8
ВР1	Тема 5. Розповсюджені типи захистів та їх недоліки. Основні вимоги до розробки систем захисту. Розповсюджені типи захистів та їх недоліки	8
ВР1	Тема 6. Засоби подолання систем захисту. Проблема існування засобів зламу захистів програмного забезпечення. Класифікація засобів подолання систем захисту програмного забезпечення. Програми розпакування, дешифрування та криптоаналізу.	8
ВР1	Тема 7. Основні поняття ОС, необхідні для створення систем захисту. Склад операційної системи. BIOS. CMOS. Переривання, їх роль і процедура звертання в програмах. Робота з дисками на фізичному рівні.	8
ВР1	Тема 8. Загальні принципи захисту програм від несанкціонованого дослідження. Принципи побудови систем захисту та їх функції. Основні методи та засоби дослідження програм. Способи вбудовування захисних механізмів в програмне забезпечення. Структура програм, захищених від дослідження.	8
ВР2-1	Тема 9. Захист від дизасемблювання. Необхідність і доцільність захисту від дизасемблювання. Основні методи протидії дизасемблюванню програм. Поняття обфускації та його види.	8
ВР1	Тема 10. Захист від несанкціонованого налагоджування Огляд і класифікація налагоджувачів. Захист від налагоджувачів реального режиму. Боротьба з налагоджувачами захищеного режиму. Додаткові прийоми антиналагоджувального програмування.	8
	ПРАКТИЧНІ ЗАНЯТТЯ	40
ВР2	Практична робота №1 Тема: Розмежування повноважень користувачів на основі паролльної аутентифікації.	12

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
	<u>Мета роботи:</u> Розробка програми розмежування повноважень користувачів на основі парольної аутентифікації. <u>Завдання:</u> Розробити програму розмежування повноважень користувачів на основі парольної аутентифікації.	
ВР2	Практична робота №2 Тема: Логування дій користувачів у програмних системах. <u>Мета роботи:</u> Засвоїти методику та отримати практичні навички розробки процедур логування дій користувачів на прикладі підсистем ідентифікації та аутентифікації користувачів із важкооборотними однонапрямленими хеш-функціями. <u>Завдання:</u> Удосконалити розроблену лабораторній роботі № 1 програмну систему з метою покращення функції ідентифікації та аутентифікації користувачів.	14
ВР2	Практична робота №3 Тема:Методи захисту програмного забезпечення. <u>Мета роботи:</u> Одержати практичні навички реалізації алгоритмів захисту програмного забезпечення для найпоширеніших моделей розповсюдження. <u>Завдання:</u> 1.Розробити програмний продукт (або удосконалити ПЗ розроблене в попередніх лабораторних роботах), що виконує мінімум 10 функцій (для прикладу - відкриття файлу, збереження файлу, довідка, друк, перегляд параметрів файлу, пошук та інші).	14
РАЗОМ		120

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 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;
практичні	контрольні завдання за кожною темою	виконання завдань під час практичних занять		виконання ККР під час заліку за бажанням студента

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 заліку 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.

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
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	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	80-84

Опис кваліфікаційного рівня	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показник оцінки
широких або мультидисциплінарних контекстах; – здатність розв’язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	неточності при реалізації двох вимог	
	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). <i>Мова:</i> – правильна; – чиста; – ясна; – точна; – логічна; – виразна; – лаконічна. <i>Комунікаційна стратегія:</i> – послідовний і несуперечливий розвиток думки; – наявність логічних власних суджень; – доречна аргументації та її відповідність 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	95-100
	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	70-73

Опис кваліфікаційного рівня	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показник оцінки
	вимог)	
	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
<i>Відповідальність і автономія</i>		
<ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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 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: MSOffice 365, MS Teams, дистанційна платформа Moodle.

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Дудатьєв А.В. Захист програмного забезпечення. Частина 1 : навчальний посібник / А.В. Дудатьєв, В.А. Каплун, В.П. Семеренко. – Вінниця : ВНТУ, 2005. – 140 с.
2. Захист програмного забезпечення. Частина 2 : навчальний посібник / В.А. Каплун, О.В. Дмитришин, Ю.В. Баришев – Вінниця : ВНТУ, 2014 . – 105 с.
3. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. – К.: Видавництво НА СБ України, 2020. – 256 с.
4. DowdM., McDonaldJ., Schuh J. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities/ Mark Dowd, JohnMcDonald, Justin Schuh —Addison-Wesley Professional, 2006. —1174 p.
5. Nadalin Alessandro. WASEC: Web Application Security for the everyday software engineer: Everything a web developer should know about application security: concise, condensed and made to last/ A. Nadalin. — Leanpub, 2020. — 161 p.— ISBN 1670062449, 9781670062444.
6. Xie M. Computing System Reliability: Models and Analysis / M.Xie, K.-L.Poh, Y.-S.Dai –Springer Science&Business Media, 2007 – 293 p.

Навчальне видання

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Програмні методи захисту інформації» для магістрів
галузі знань 12 Інформаційні технології**

**Розробник:
Сафаров Олександр Олександрович**