

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

Кафедра вищої математики

«ЗАТВЕРДЖЕНО»

завідувач кафедри

Сдвижкова О.О. _____

« ____ » _____ 20 ____ року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Прикладна криптологія»

Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітній рівень.....	Бакалавр
Освітньо-професійна програма	Кібербезпека
Статус	нормативна
Загальний обсяг	9 кредитів ЄКТС (270 годин)
Форма підсумкового контролю	Іспит
Термін викладання	5-6-й семестр
Мова викладання	українська

Викладачі: доц. Бабець Д.В.

Пролонговано: на 2019__/2020__ н.р. _____ (_____) «__» ____ 2019__ р.
(підпис, ПІБ, дата)

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

Дніпро
НТУ «ДП»
2019

Робоча програма навчальної дисципліни «Прикладна криптологія» для бакалаврів спеціальності 125 Кібербезпека / Нац. техн. ун-т. «Дніпровська політехніка», кафедра вищої математики – Д.: НТУ «ДП», 2019. – 12 с.

Розробник – Бабець Д.В.

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.

Робоча програма буде у пригоді для формування змісту підвищення кваліфікації науково-педагогічних працівників кафедр університету.

Погоджено рішенням методичної комісії спеціальності 125 «Кібербезпека» (протокол № від _____).

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.....	5
6 ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ	6
6.1 Шкали	6
6.2 Засоби та процедури.....	7
6.3 Критерії.....	8
7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ	11
8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ.....	122

1. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

В освітньо-професійній програмі Національного технічного університету «Дніпровська політехніка» спеціальності 125 Кібербезпека здійснено розподіл програмних результатів навчання (ПРН) за організаційними формами освітнього процесу. Зокрема, до дисципліни Ф13 «Прикладна криптологія» віднесено такі результати навчання:

CP5	аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації;
-----	--

Мета дисципліни – надати фундаментальні знання з математичних основ криптографічного захисту інформації, необхідні відомості з теорії чисел, навчити студентів правильно проводити аналіз погроз безпеці інформації, основним методам, механізмам, алгоритмам та протоколам криптографічного захисту інформації, а також методам проведення криптографічного аналізу.

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
РН	CP5	аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації

3. БАЗОВІ ДИСЦИПЛІНИ

Назва дисципліни	Здобуті результати навчання
Б1 Вища математика	Застосування теорії, принципів, методів й понять фундаментальних і загально-інженерних наук під час опанування спеціальних дисциплін та діяльності за фахом
Б3 Теорія ймовірностей та математична статистика	Виконувати аналіз ймовірнісних подій і функцій
	Вирішувати типові задачі математичної статистики для вихідних умов різної розмірності

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

Вид навчальних занять	Обсяг, години	Розподіл за формами навчання, години					
		денна		вечірня		заочна	
		аудиторні заняття	самостійна робота	аудиторні заняття	самостійна робота	аудиторні заняття	самостійна робота
лекційні	135	60	75			-	-
практичні	135	60	75			-	-
лабораторні	-	-	-	-	-	-	-
семінари	-	-	-	-	-	-	-
РАЗОМ	270	120	150	-	-	-	-

5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
	ЛЕКЦІЇ	60
CP5тп1	1. Відомості з теорії чисел та математичні основи криптографії	14
	Складність арифметичних дій. Алгоритм Евкліда і його складність. Прості числа. Числа Марсена. Числа Ферма.	
	Функція Ейлера. Властивості функції Ейлера. Теорема Ейлера.	
	Алгебраїчні порівняння с одним невідомим. Розв'язок лінійних порівнянь. Системи порівнянь першого степеню. Китайська теорема про лишки.	
	"Класична" криптографія. Класичні криптосистеми та їх криптоаналіз	
CP5тп2	2. Симетричні криптографічні системи	12
	Криптографічна стійкість шифру. Симетричні криптографічні перетворення та їх властивості	
	Сучасні стандарти симетричного шифрування. DES	
	Схеми шифрування ГОСТ 28147-89 і Rijndael	
	Режими шифрування. Задачі режиму шифрування	
	Джерела ключів та ключової інформації, вимоги до них	
CP5тп3	3. Асиметричні криптосистеми та їх крипто аналіз	18
	Вступ в теорію асиметричних крипто перетворень. Схеми Діффі – Хелмана.	
	Криптосистема RSA. Методи крипто аналізу.	
	Джерела ключів асиметричних криптосистем та вимоги до них.	
	Криптосистема Ель Гамала. Проблема дискретного логарифмування	
	Асиметричні криптоперетворення в групах точок еліптичних кривих	
CP5тп4	4. Криптографічні механізми та протоколи	16
	Забезпечення цілісності і авторства в електронному документообігу.	
	Функції хешування	
	Стандарти алгоритмів формування і перевірки ЕЦП	
	Криптографічні механізми та протоколи управління ключами	
	Криптографічні механізми та протоколи автентифікації.	
	Механізми розподілення таємниці	
	Синтез та аналіз криптографічних протоколів	
	ПРАКТИЧНІ ЗАНЯТТЯ	60
	1. Алгоритм Евкліда. Знаходження НСД та НСК.	2
	2. Бінарний алгоритм піднесення у степінь за модулем.	2
	3. Функція Ейлера.	2
	4. Алгоритм знаходження оберненого елемента за модулем.	2
	5. Прості числа.	2
	6. Розв'язок лінійних порівнянь.	2
	7. Розв'язок систем порівнянь першого степеню.	2

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
	8. Моноалфавітні підстановки та їх криптоаналіз.	2
	9. Шифр Хілла та його криптоаналіз.	2
	10. Криптографічна стійкість шифру.	2
	11. Ймовірнісна модель шифру за Шеноном. Шифр Вернама.	2
	12. Мережа Фейстеля.	2
	13. Стандарт DES.	2
	14. Скінченні поля. Поле Галуа.	2
	15. Сучасний стандарт симетричного шифрування AES.	2
	16. Схема Діффі-Хелмана. Первісні корені.	2
	17. Алгоритм асиметричної криптографії RSA.	2
	18. Крипто аналіз RSA.	2
	19. Криптосистема Ель Гамала.	2
	20. Пошук дискретного логарифму. Алгоритм Шенкса.	2
	21. Електронний цифровий підпис. ЕЦП.	2
	22. Електронний цифровий підпис та Ель Гамала (EGSA).	2
	23. ЕЦП за схемою DSS.	2
	24. Поділ секрету. Гранична схема Блеклі.	2
	25. Поділ секрету. Гранична схема Шаміра.	2
	26. Основи побудови еліптичних кривих.	2
	27. Криптосистема Ель-Гамала над групою точок еліптичної кривої (EC-El-Gamal).	2
	28. Електронний цифровий підпис над групою точок еліптичної кривої (ECDSA).	2
	29. Керування ключами.	2
	30. Стеганографія.	2
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 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 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, комунікації, автономності та відповідальності студента за вимогами НРК до 7-го кваліфікаційного рівня під час демонстрації регламентованих робочою програмою результатів навчання.

Студент на контрольних заходах має виконувати завдання, орієнтовані виключно на демонстрацію дисциплінарних результатів навчання (розділ 2).

Засоби діагностики, що надаються студентам на контрольних заходах у вигляді завдань для поточного та підсумкового контролю, формуються шляхом конкретизації вихідних даних та способу демонстрації дисциплінарних 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	модульна контрольна робота	визначення середньозваженого результату поточних контролів; виконання екзаменаційної роботи
практичні	контрольні завдання за кожною темою	виконання завдань під час практичних занять		
	або 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 або індивідуального завдання.

Якщо зміст певного виду занять підпорядковано декільком дескрипторам, то інтегральне значення оцінки може визначатися з урахуванням вагових коефіцієнтів, що встановлюються викладачем.

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 залікову роботу, яка містить завдання, що охоплюють ключові дисциплінарні результати навчання.

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

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

Інтегральне значення оцінки виконання контрольного завдання може визначатися з урахуванням вагових коефіцієнтів, що встановлюється кафедрою для кожного дескриптора НРК.

6.3 Критерії

Реальні результати навчання студента ідентифікуються та вимірюються відносно очікуваних під час контрольних заходів за допомогою критеріїв, що описують дії студента для демонстрації досягнення результатів навчання.

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 бакалаврського рівня вищої освіти (подано нижче).

Таблиця 1 – Загальні критерії досягнення результатів навчання для 7-го кваліфікаційного рівня за НРК (бакалавр)

Інтегральна компетентність – здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у певній галузі професійної діяльності або у процесі навчання, що передбачає застосування певних теорій та методів відповідної науки і характеризується комплексністю та невизначеністю умов.

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
Знання		
- концептуальні знання, набуті у	Відповідь відмінна – правильна, обґрунтована, осмислена. Характеризує наявність:	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
процесі навчання та професійної діяльності, включаючи певні знання сучасних досягнень; -критичне осмислення основних теорій, принципів методів і понять у навчанні та професійній діяльності	- концептуальних знань; - високого ступеню володіння станом питання; - критичного осмислення основних теорій, принципів, методів і понять у навчанні та професійній діяльності Відповідь містить негрубі 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		
-розв'язання складних непередбачуваних задач і проблем у спеціалізованих сферах професійної діяльності та/або навчання, що передбачає збирання та інтерпретацію інформації (даних), вибір методів та інструментальних засобів, застосування інноваційних підходів	Відповідь характеризує уміння: виявляти проблеми; формулювати гіпотези; розв'язувати проблеми; обирати адекватні методи та інструментальні засоби; збирати та логічно й зрозуміло інтерпретувати інформацію; використовувати інноваційні підходи до розв'язання завдання	95-100
	Відповідь характеризує уміння застосовувати знання в практичній діяльності з негрубими помилками	90-94
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації однієї вимоги	85-89
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації двох вимог	80-84
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації трьох вимог	74-79
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації чотирьох вимог	70-73
	Відповідь характеризує уміння застосовувати знання в практичній діяльності при виконанні завдань за зразком	65-69
	Відповідь характеризує уміння застосовувати знання при виконанні завдань за зразком, але з неточностями	60-64
	Рівень умінь незадовільний	<60
Комунікація		
-донесення до фахівців і	Вільне володіння проблематикою галузі. - Зрозумілість відповіді (доповіді). - Мова:	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
нефахівців інформації, ідей, проблем, рішень та власного досвіду в галузі професійної діяльності; здатність ефективно формувати комунікаційну стратегію	- 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; - доречна техніка відповідей на запитання; - здатність робити висновки та формулювати пропозиції	
	Достатня зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія з незначними хибами	90-94
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано три вимоги))	85-89
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано чотири вимоги)	80-84
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано п'ять вимог)	74-79
	Задовільне володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано сім вимог)	70-73
	Часткове володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано дев'ять вимог)	65-69
	Фрагментарне володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано 10 вимог)	60-64
	Рівень комунікації незадовільний	<60
Автономність та відповідальність		
-управління комплексними діями або	Відмінне володіння компетенціями менеджменту особистості, орієнтованих на: 1) управління комплексними проектами, що передбачає:	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
проектами, відповідальність за прийняття рішень у непередбачуваних умовах; -відповідальність за професійний розвиток окремих осіб та/або груп осіб; -здатність до подальшого навчання з високим рівнем автономності	- дослідницький характер навчальної діяльності, позначена вмінням самостійно оцінювати різноманітні життєві ситуації, явища, факти, виявляти і відстоювати особисту позицію; - здатність до роботи в команді; - контроль власних дій; 2) відповідальність за прийняття рішень в непередбачуваних умовах, що включає: - обґрунтування власних рішень положеннями нормативної бази галузевого та державного рівнів; - самостійність під час виконання поставлених завдань; - ініціативу в обговоренні проблем; - відповідальність за взаємовідносини; 3) відповідальність за професійний розвиток окремих осіб та/або груп осіб, що передбачає: - використання професійно-орієнтованих навичок; - використання доказів із самостійною і правильною аргументацією; - володіння всіма видами навчальної діяльності; 4) здатність до подальшого навчання з високим рівнем автономності, що передбачає: - ступінь володіння фундаментальними знаннями; - самостійність оцінних суджень; - високий рівень сформованості загальнонавчальних умінь і навичок; - - самостійний пошук та аналіз джерел інформації	
	Упевнене володіння компетенціями менеджменту особистості (не реалізовано дві вимоги)	90-94
	Добре володіння компетенціями менеджменту особистості (не реалізовано три вимоги)	85-89
	Добре володіння компетенціями менеджменту особистості (не реалізовано чотири вимоги)	80-84
	Добре володіння компетенціями менеджменту особистості (не реалізовано шість вимог)	74-79
	Задовільне володіння компетенціями менеджменту особистості (не реалізовано сім вимог)	70-73
	Задовільне володіння компетенціями менеджменту особистості (не реалізовано вісім вимог)	65-69
	Рівень автономності та відповідальності фрагментарний	60-64
	Рівень автономності та відповідальності незадовільний	<60

7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Технічні засоби навчання.

Дистанційна платформа Moodle.

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна

1. Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я Фомичова // Математичні основи криптографії / Дніпропетровськ. НГУ. 2004.
2. С.О. Сушко, Г.В. Кузнецов, Л.Я Фомичова, А.В. Корабльов // Математичні основи криптоаналізу / Дніпропетровськ. НГУ. 2010
3. Криптологія в тестах, задачах і прикладах: Навчальний посібник ./ Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомичова.- Д.:Національний гірничий університет, 2013.-318 с.

Допоміжна

1

1. О. В. Вербіцкий Вступ до криптології. ВНТА. Львів.1998 – 247с.
2. Н. Коблиц. Курс теории чисел и криптографии. М.: ТВП, 2001.
3. О. Н. Василенко. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003.
4. А. В. Черемушкин. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002.
5. А. А. Болотов, С. Б. Гашков, А. Б. Фролов, А. А. Часовских. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. М.: 2006.
6. Б. Анин Защита компьютерной информации СПб: БХВ – Санкт-Петербург. 2000. –384с.
7. Б. С.Люцарев, К. В. Ермаков, Е. Б. Рудный, И. Е. Ермаков. Безопасность компьютерных сетей на основе Windows NT. 1998. – 340с. «Channel Tr. Ltd»
8. В. В. Домарев Защита информации и безопасность компьютерных систем. Diasoft. Киев. 1999. –453с.
9. В. Ємець, А. Мельник, Р. Попович. Сучасна криптографія. Основні поняття. Львів-2003, “Бак”, -144с.
10. Т. Корнієнко, А. Мельник, В. Мельник. Алгоритм та процеси симетричного блокового шифрування. Львів-2003, “Бак”, -168с.