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

Кафедра безпеки інформації та телекомунікацій

«ЗАТВЕРДЖЕНО»
на засіданнікафедри БІТ

(протокол № 9 від 23.04.2019 р.)

завідувач кафедри
Корнієнко В.І. _____

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Методи побудови і аналізу криптосистем»

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

Викладачі: ст. в. Саксонов Г.М..

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

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

Дніпро
НТУ «ДП»
2019

Робоча програма навчальної дисципліни «Методи побудови і аналізу криптосистем» для магістрів спеціальності 125 «Кібербезпека» / Нац.техн. ун-т. «Дніпровська політехніка», каф. безпеки інформації та телекомунікацій – Д. : НТУ «ДП», 2019. – 13 с.

Розробник – Саксонов Г.М.

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 в пригоді для формування змісту підвищення кваліфікації науково-педагогічних працівників кафедр університету.

Погоджено рішенням методичної комісії спеціальності 125 «Кібербезпека» (протокол № 9 від 23.04.2019 р.).

ЗМІСТ

1 МЕТА НАВЧАЛЬНОЇ ДИЦИПЛІНИ 4
2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ 4
3 БАЗОВІ ДИСЦИПЛІНИ 4
4 ОБСЯГ І РОЗПОДІЛ ЗА ФОРМАМИ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ТА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ 5
5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ 5
6 ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ 7
6.1 Шкали 7
6.2 Засоби та процедури 7
6.3 Критерії 9
7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ 12
8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ 12

1 МЕТА НАВЧАЛЬНОЇ ДИЦИПЛІНИ

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 Ф1 «Методи побудови і аналізу криптосистем» віднесено такі результати навчання:

ЗР2	Використовувати методи фундаментальних наук та загально інженерних наук для розв'язання загально інженерних , професійних та наукових задач.
СР1	Використовуватиуправлінсько-організаційні та правові методи, засоби й заходи для реалізації проектних рішень з побудови систем забезпечення інформаційної та кібернетичної безпеки.

Мета дисципліни– надати теоретичні та практичні знання математичних основ побудови та криптоаналізу, сучасних методів пошуку вразливостей криптоалгоримтів та протоколів, оцінки криптостійкості алгоритмів шифрування.

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**
СР1	СР1-Ф1	Використовувати управлінсько-організаційні та правові методи, засоби й заходи для реалізації проектних рішень з побудови систем забезпечення інформаційної та кібернетичної безпеки.
ЗР2	ЗР2-Ф1	Використовувати методи фундаментальних наук та загально інженерних наук для розв'язання загально інженерних , професійних та наукових задач.

3 БАЗОВІ ДИСЦИПЛІНИ

Назва дисципліни	**Здобуті результати навчання**
Ф2 Спеціальні розділи з математики	аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації
Ф13 Прикладна криптологія	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації
Ф16 Цифрова стеганографія	забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах

Назва дисципліни	Здобуті результати навчання
В 2.12 Цифрові методи обробки інформації	забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах

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	90	26	64	-	-	-	-
практичні	90	26	64	-	-	-	-
лабораторні	-	-	-	-	-	-	-
семінари	-	-	-	-	-	-	-
РАЗОМ	180	52	128	-	-	-	-

5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Шифри ДРН	**Види та тематика навчальних занять**	**Обсяг складових,** *години (ауд./сам.роб)*
	ЛЕКЦІЇ	**26/64**
СР1-Ф1 ЗР2-Ф1	**1 Криптосистеми.** 1.1Класифікація . 1.2 Елементи криптосистем	12
СР1-Ф1 ЗР2-Ф1	**2 Криптографічні протоколи** 2.1. Види криптографічних протоколів 2.2 Свойства. що визначають безпеку протоколів. 2.3 Атаки на протоколи. 2.4 Аналіз і моделювання протоколів	10
СР1-Ф1 ЗР2-Ф1	**3 Принципи та структура ключових систем** 3.1. Управління ключами 3.2. Розподіл секретних ключів за допомогою системи з відкритим ключем 3.3. Обмін ключами за схемою Діффі-Хеллмана	14
СР1-Ф1 ЗР2-Ф1	**4 Аутентифікація** 4.1 Основні поняття 4.2. Вимоги аутентифікації	10
СР1-Ф1 ЗР2-Ф1	**5 Парольна аутентифікація** 5.1.Функції парольної автентифікації	8
СР1-Ф1 ЗР2-Ф1	**6 Методи аутентифікації повідомлень** **6.1.** Аутентифікація повідомлень і функції хешування 6.2. Код автентичності повідомлення	6
СР1-Ф1 ЗР2-Ф1	**7 Протоколи цифрового підпису** 7.1. Цифрові підписи 7.2. Стандарт цифрого підпису DSS	6

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, *години (ауд./сам.роб)*
ЗР2-Ф1	**8 Реалізація криптографічних алгоритмів. Використання криптографічних функцій CryptoAPI** 8.1. Будова і можливості CryptoAPI 8.2. Криптопровайдери 8.3. Контейнери ключів 8.3. Сертифікати 8.4. Алгоритми	8
СР1-Ф1 ЗР2-Ф1	**9 Основи технології Blockchain** 9.1. Принципи технології довіри. Структура блоку. Заголовок блоку. Блок генезису. 9.2. Алгоритми доказу виконаної роботи.	10
	ПРАКТИЧНІ ЗАНЯТТЯ	**26/64**
СР1-Ф1 ЗР2-Ф1	1. Подання криптографічних протоколів .Проста система цифрового підпису	8/20
СР1-Ф1	2. Криптосистема аутентифікації з одноразовими числами. Криптосистема аутентифікації «запросити відповідь»	10/24
ЗР2-Ф1	3. Робота з криптографічними функціями CryptoAPI	8/20
	РАЗОМ	**52/128**

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 8-го кваліфікаційного рівня під час демонстрації регламентованих робочою програмою результатів навчання.

Студент на контрольних заходахмає 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

<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="3">комплексна контрольна робота (ККР)</td><td rowspan="3">визначення середньозваженого результату поточних контролів;

виконання ККР під час екзамену за бажанням студента</td></tr>
<tr><td rowspan="2">практичні</td><td>контрольні завдання за кожною темою</td><td>виконання завдань під час практичних занять</td></tr>
<tr><td>або індивідуальне завдання</td><td>виконання завдань під час самостійної роботи</td></tr>
</table>

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 екзамену має право виконувати ККР, яка містить завдання, що охоплюють ключові дисциплінарні результати навчання.

Кількість конкретизованих завдань ККР повиннавідповідати 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.

Інтегральне значення оцінки виконання ККР 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 компетентністні характеристики, визначені НРК для магістерського рівня вищої освіти (подано нижче).

Загальні критерії досягнення результатів навчання для 8-го кваліфікаційного рівня за НРК

Інтегральна компетентність – здатність розв'язувати складні задачі і проблеми у певній галузі професійної діяльності або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
Знання		
♦ спеціалізовані	Відповідь відмінна – правильна, обґрунтована,	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
концептуальні знання, набуті у процесі навчання та/або професійної діяльності на рівні новітніх досягнень, які є основою для оригінального мислення та інноваційної діяльності, зокрема в контексті дослідницької роботи; ♦ критичне осмислення проблем у навчанні та /або професійній діяльності та на межі предметних галузей	осмислена. Характеризує наявність: - спеціалізованих концептуальних знань на рівні новітніх досягнень; - критичне осмислення проблем у навчанні та/або професійній діяльності та на межі предметних галузей	
	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 задач і проблем, що потребує оновлення та інтеграції знань, часто в умовах неповної/недостатньої інформації та суперечливих вимог; ♦ провадження дослідницької та/або інноваційної діяльності	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 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		

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
♦ зрозуміле і недвозначне донесення власних висновків, а також знань та пояснень, що їх обґрунтовують, до фахівців і нефахівців, зокрема до осіб, які навчаються; ♦ використання іноземних мов у професійній діяльності	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; - 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 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
Автономність та відповідальність		
♦ відповідальність за розвиток професійного знання і практик, оцінку стратегічного розвитку команди; ♦ здатність до	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);	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
подальшого навчання, яке значною мірою є автономним та самостійним	- 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	
	Упевнене володіння компетенціями автономності та відповідальності з незначними хибами	90-94
	Добре володіння компетенціями автономності та відповідальності (не реалізовано дві вимоги)	85-89
	Добре володіння компетенціями автономності та відповідальності (не реалізовано три вимоги)	80-84
	Добре володіння компетенціями автономності та відповідальності (не реалізовано чотири вимоги)	74-79
	Задовільне володіння компетенціями автономності та відповідальності (не реалізовано п’ять вимог)	70-73
	Задовільне володіння компетенціями автономності та відповідальності (не реалізовано шість вимог)	65-69
	Задовільне володіння компетенціями автономності та відповідальності (рівень фрагментарний)	60-64
	Рівень автономності та відповідальності незадовільний	<60

7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Технічні засоби навчання.

Спеціалізовані програмні продукти.

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Тилборг ван Х.К.А. Основыкриптологии /Тилборг ван Х.К.А. – М.: Мир, 2006. – 471 с.

2. Защитаинформации в системах телекомуникации: Учебноепособие для вузов / [Банкет В.Л. и др.]. – Од., УГАС им. А.С. Попова, 1997. – 96 с.

3. Гулак Г. Різні підходи до визначення випадкових послідовностей: /Г.Гулак. Л.Ковальчук// Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – 2001. - №3 – С. 127-133.

4. Б. ШнайерПрикладнаякриптография. Теория и практика/ Венбо Мао; [пер. с англ.] . – М.: Изд.дом «Вильямс». 2005. – 786 с.

5. Бессалов А.В. Криптосистемы на эллиптических кривых / А.В. Бессалов, А.Б. Телиженко. – К.: ІВЦ Видавництво «Політехніка», 2004. – 224.

6. Вербицький О. Вступ до криптології/ Вербицький О. – Львів : Видавництво науково- технічної літератури, 1998. – 247 с.

7.Dolev D., Yao A. *Onthesecurityofpublickeyprotocols*. IEEE Trans. onInf. Theory. 29 (2), 1983, 198–208.

8.Millen J. K., Clark S. C., Freedman S. B. *TheInterrogator: protocolsecurityanalysis.* IEEE Trans. onSoftwareEngineering, SE-13 (2), 1987.

9.Longley D., Rigby S. *Anautomaticsearchforsecurityflawsinkeymanagementschemes.* Computersandsecurity, 11 (1), 1992, 75–90.

10.Burrows M., Abadi M., Needham R. *A logicofauthentication.* ACM Trans. inComputerSystems, 8 (1), 1990, 18–36.

Навчальне видання

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Методи і аналіз криптологічнихситем» для магістрів спеціальності 125 «Кібербезпека»

Розробник: Геннадій Михайлович Саксонов