СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Методи побудови і аналізу криптосистем»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**Ступінь освіти**	магістр
	Освітня програма	Кібербезпека
	Тривалість викладання	3,4 чверті
	Заняття:	Весняний семестр
	лекції:	2 години
	практичні заняття:	2 години
	Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»:

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладача:

Саксонов Генадій Михайлович	ст.викладач
Персональна сторінка	http://bit.nmu.org.ua/ua/pro_kaf/prepods/saksonov.php
E-пошта:	Saksonov.h.m@nmu.one

1. Анотація до курсу

Криптографія – до 70-х рр. XX ст. – галузь науки і практичної діяльності, пов'язана з розробкою, застосуванням і аналізом шифросистем. В даний час криптографія – галузь науки, техніки і практичної діяльності, пов'язана з розробкою, застосуванням і аналізом криптографічних систем захисту інформації. Основними функціями криптографічних систем є забезпечення конфіденційності і аутентифікації різних аспектів інформаційної взаємодії. Джерелом загроз при вирішенні криптографічних завдань вважаються навмисні дії противника або несумлінного учасника інформаційної взаємодії, а не випадкові спотворення інформації внаслідок перешкод, відмов і т. п. Курс «Методи побудови і аналізу криптосистем» може вивчатися як окрема дисципліна, або як складова частина більш загального курсу, яка розкриває варіанти визначення основних криптографічних понять, заснованих на введенні узагальнюючого поняття криптосистеми. Визначаються види криптографічних систем, основними з яких є системи шифрування, ідентифікації, імітозащіти, цифрового підпису, і ключова система, що забезпечує роботу інших систем..

2. Мета та завдання курсу

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

Завдання: отримання теоретичних та практичних знань, щодо побудови та аналізу криптографічних систем, уміння їх застосовувати в процесі професійної діяльності.

3. Результати навчання

Використовувати математичні та технічні методи, засоби й заходи для реалізації проектних рішень з побудови систем та методів криптоаналізу.

Використовувати різні сучасні інформаційні технології та проводити криптоаналіз відомих шифрів.

Подавати криптографічні протоколи та систему цифрового підпису.

Реалізовувати різні криптографічні алгоритми та криптографічні функції CryptoAPI.

4.Структура курсу

ЛЕКЦІЇ

1 Криптосистеми.

1.1Класифікація .

1.2 Элементи криптосистем

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

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

4 Аутентифікація
4.1 Основні поняття
4.2. Вимоги аутентифікації

5 Парольна аутентифікація
5.1.Функції парольної автентифікації

6 Методи аутентифікації повідомлень
6.1. Аутентифікація повідомлень і функції хешування
6.2. Код автентичності повідомлення

7 Протоколи цифрового підпісу
7.1. Цифрові підписи

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

9 Основи технології Blockchain
9.1. Принципи технології довіри. Структура блоку. Заголовок блоку. Блок генезису.
9.2. Алгоритми доказу виконаної роботи.

ПРАКТИЧНІ ЗАНЯТТЯ

1.Подання криптографічних протоколів .Проста система цифрового підпису.
2. Криптосистема аутентифікації з одноразовими числами. Криптосистема аутентифікації «запросити відповідь»
3. Робота з криптографічними функціями CryptoAPI

5. Технічне обладнання та/або програмне забезпечення

Необхідний доступ до системи дистанційного навчання НТУ «ДП». Активований акаунт університетської пошти (student.i.p.@nmu.one) на Офіс365.

Технічне обладнання до практичних робіт:

№ роботи	Назва роботи	Інструменти, обладнання та програмне забезпечення, що застосовуються при проведенні роботи
1	1. Подання криптографічних протоколів .Проста система цифрового підпису	Компілятор C\C++
3	Робота з криптографічними функціями CryptoAPI	Компілятор C\C++

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

6.2. Оцінка виставляється на основі двох теоретичних модулів та трьох практичних робіт. Максимальний бал за кожний теоретичний модуль складає 20 балів (2 теоретичні питання по 10 балів). Кожна з практичних робіт оцінюється в 10 балів.

Критерії оцінювання

Реальні результати навчання студентаідентифікуються 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.

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

	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: 1. спеціалізованих концептуальних знань на рівні новітніх досягнень; 2. 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: 3. виявляти проблеми; 4. формулювати гіпотези; 5. розв’язувати проблеми; 6. оновлювати знання; 7. інтегрувати знання; 8. провадити інноваційну діяльність; 9. 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	74-79

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники 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	застосовувати знання в практичній діяльності, але має певні неточності при реалізації трьох вимог	
	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:* 10. правильна; 11. чиста; 12. ясна; 13. точна; 14. логічна; 15. виразна; 16. лаконічна. *Комунікаційна стратегія:* 17. послідовний і несуперечливий розвиток думки; 18. наявність логічних власних суджень; 19. доречна аргументації та її відповідність відстоюваним положенням; 20. правильна структура відповіді (доповіді); 21. правильність відповідей на запитання; 22. доречна техніка відповідей на запитання; 23. здатність робити висновки та формулювати пропозиції; 24. 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	85-89

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники оцінки
	три вимоги)	
	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: 25. використання принципів та методів організації діяльності команди; 26. ефективний розподіл повноважень в структурі команди; 27. підтримка врівноважених стосунків з членами команди (відповідальність за взаємовідносини); 28. стресовитривалість; 29. саморегуляція; 30. трудова активність в екстремальних ситуаціях; 31. високий рівень особистого ставлення до справи; 32. володіння всіма видами навчальної діяльності; 33. належний рівень фундаментальних знань; 34. належний рівень сформованості загальнонавчальних умінь і навичок	95-100
	Упевнене володіння компетенціямивідповідальності 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

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники 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. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

7.6. Бонуси

За активність та правильні відповіді на лекційних та практичних заняттях студент може отримати до +2 балів до семестрової оцінки на кожному занятті.

8. Рекомендовані джерела інформації

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

2. Защита информации в системах телекомуникации: Учебное пособие 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.

3. Б. Шнайер Прикладная криптография. 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. Саксонов Г.М.,Жукова О. А. КОНСПЕКТ ЛЕКЦІЙ з дисципліни «Методи побудови і аналізу криптосистем» для магістрів спеціальності 125 Кібербезпека галузі знань 12 Інформаційні технології. – Дніпро.: Національний технічній університет «Діпровська політехніка». 2019. – 37 с.

8. Саксонов Г.М.,Жукова О. А.МЕТОДИЧНІ ВКАЗІВКИ до виконання лабораторних робіт з дисципліни «Методи побудови і аналізу криптосистем» для магістрів спеціальності 125 Кібербезпека галузі знань 12 Інформаційні технології. – Дніпро.: Національний технічній університет «Діпровська політехніка». 2019. – 29 с.

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

10.Millen J. K.,Clark S. C.,Freedman S. B. The Interrogator: protocol security analysis. IEEE Trans. onSoftwareEngineering, SE-13 (2), 1987.

11.Longley D.,Rigby S. Anautomatic search forsecurity flaw sinkey managements chemes. Computersan dsecurity, 11 (1), 1992, 75–90.

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