МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ
Факультет № 4
Кафедра протидії кіберзлочинності

ЗАТВЕРДЖЕНО
На спільному засідання кафедри протидії кіберзлочинності факультету №4 та кафедри кібербезпеки та DATA-технологій факультету №6
протокол № 2 від 22.06.2023
Завідувач кафедри
Олександр МАНЖАЙ
_____

ПРИКЛАДНА КРИПТОЛОГІЯ (ОК.16)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Кафедра протидії кіберзлочинності (https://univd.edu.ua/uk/dir/1740/kafedra-protydii-kiberzlochynnosti)
Контактний телефон	+38 057 7398085 (роб.)
E-mail	kaf-itk@univd.edu.ua
ЛЕКТОР (ЛЕКТОРИ)	
	**Носов Віталій Вікторович,** професор кафедри протидії кіберзлочинності факультету № 4, кандидат технічних наук, доцент E-mail: vitnos@univd.edu.ua **Лекційний потік:** факультет № 4, Ф4-302
Назва освітньо-професійної програми	Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем) Cybersecurity and information protection (security of information and communication systems)
Рівень вищої освіти	Перший (бакалаврський) (НРК України – 6 рівень та перший цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технології

Спеціальність	125 Кібербезпека та захист інформації
Статус дисципліни	Нормативна компонента освітньо-наукової програми, вивчається в 5, 6 семестрах 3 курсу навчання
Мета вивчення дисципліни	ознайомлення з теоретичними основами криптографії та прикладними аспектами її застосування
Завдання вивчення дисципліни	- закладання основ знань та умінь використання криптографічних і стеганографічних систем; - формування навичок аналізу та застосування криптографічних систем і протоколів при забезпеченні кібербезпеки.
Обсяг дисципліни в кредитах ECTS/годинах	8 кредитів ECTS (загальний обсяг – 240 год.) З них (денна/заочна):
	- аудиторна робота: 120/24 год.
	- самостійна робота: 120/216 год.
Форми та види проведення навчальних занять	Форма навчання – денна/заочна Види навчальних занять: - лекції: 60/8 год.; - лабораторні заняття: 60/16 год.
Самостійна робота	Опрацювання рекомендованої літератури, виконання домашніх завдань до лабораторних занять, виконання індивідуальних завдань до лабораторних занять
Індивідуальні завдання	Наукові доповіді, індивідуальні завдання до лабораторних занять
Необхідне обладнання	Мультимедійне обладнання (ноутбук, проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
Мова викладання	Українська
Контроль	***Методи контролю***: поточний та підсумковий контроль (залік, екзамен) ***Форми контролю***: захист індивідуальних завдань на лабораторних заняттях, тестування, перевірка аудиторних контрольних робіт, перевірка виконання самостійних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням.
Інтегральна компетентність, загальні компетентності (ЗК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або

	кібербезпеки, що характеризується комплексністю та неповною визначеністю умов ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та розуміння професії. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням
Фахові компетентності (ФК)	ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, з метою реалізації встановленої політики інформаційної та/або кібербезпеки ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ

Тема № 1. Криптосистеми з секретним ключем

Концепції шифрування з секретним ключем. Класичні шифри: Цезаря, Віженера, Вернама, Полібія, гамування. Криптоаналіз шифру Віженера. Принципи сучасної криптографії. Теоретичні основи досконалої секретності. Одноразовий блокнот (шифр Вернама). Обчислювальна секретність. Псевдовипадкові послідовності. Доказовість безпечності криптографії. Поняття дуже сильної безпеки та псевдовипадкові функції блокових шифрів. CPA-безпечні криптографічні перетворення. Chosen-Ciphertext і Padding-Oracle атаки. Коди автентифікації повідомлення. Хеш функції та шифрування з автентифікацією.

Основні параметри блокових (DES, AES, ГОСТ 28147, ДСТУ 7624) та потокових (RC4, ДСТУ 8845) стандартів шифрування.

Тема № 2. Криптосистеми з публічним ключем

Обчислення модульної арифметики (алгоритм Евкліда, теореми Ейлера, Ферма). Обчислення у скінченних алгебраїчних полях. Важкі теоретико-числові проблеми. Концепції шифрування з публічним ключем. Розподіл ключів та шифрування з публічним ключем. Генерація спільних секретів (DH). Алгоритми шифрування з публічним ключем (RSA, EG). Алгоритми цифрових підписів (DSA). Схеми ідентифікації та інфраструктура відкритих ключів.

Тема № 3. Криптографічні протоколи

Основні відомості про криптопротоколи: розподілу ключів, автентифікації сторін. Протоколи захисту мережевого трафіку IPSec. Протоколи безпечної передачі даних прикладного рівня https.

Тема № 4. Цифрова стеганографія

Поняття цифрової стеганографії. Модель стеганосистеми. Основні вимоги до стеганосистеми. Відкриті, напівзакриті, закриті стеганосистеми. Поняття ЦВЗ, класифікація. Метод модифікації найменшого значущого біта. Атаки на стеганосистеми.	
Програмні результати навчання (ПРН)	ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
	ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
	ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах
	ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем
	ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах
	ПРН 31. Застосовувати теорії та методи захисту щодо забезпечення безпеки елементів інформаційно-телекомунікаційних систем
	ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
	ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах
Критерії оцінювання результатів навчання	Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю:

	● поточний контроль - 50 балів; ● підсумковий контроль - 50 балів. Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на семінарських заняттях (здобувач має отримати не менше 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: захист звітів лабораторних робіт з коефіцієнтом 5. Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (заліку, екзамені).

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS

Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка за шкалою ECTS**	
		Оцінка	**Пояснення**
97-100	Відмінно («зараховано»)	A	**«Відмінно»** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою
94-96			
90-93			
85-89	Добре («зараховано»)	B	**«Дуже добре»** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками
80-84			

75-79		C	**«Добре»** – теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією – двома значними помилками
70 –74	Задовільно («зараховано»)	D	**«Задовільно»** – теоретичний зміст курсу освоєний не повністю, але прогалини не носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань, містять помилки, робота з трьома значними помилками
65 – 69			
60 – 64		E	**«Достатньо»** – теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального, робота, що задовольняє мінімуму критеріїв оцінки
40 – 59	Незадовільно («не зараховано»)	FX	**«Умовно незадовільно»** – теоретичний зміст курсу освоєний частково, необхідні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки
21 – 40			
1–20		F	**«Безумовно незадовільно»** – теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не призведе до значного підвищення якості виконання навчальних завдань, робота, що потребує повної переробки
Перелік питань, що виносяться на підсумковий контроль			
1. Концепції шифрування з секретним ключем. 2. Методи криптоаналізу шифру Віженера. 3. Принципи сучасної криптографії.			

4. Теоретичне обґрунтування досконалої секретності.
5. Одноразовий блокнот (шифр Вернама).
6. Обчислювальна секретність.
7. Формування псевдовипадкових послідовностей.
8. Доказовість безпечності криптографії.
9. Поняття дуже сильної безпеки
10. Псевдовипадкові функції блокових шифрів.
11. CPA-безпечні криптографічні перетворення.
12. Chosen-Ciphertext атаки на шифртекст.
13. Padding-Oracle атаки на шифртекст.
14. Коди автентифікації повідомлення.
15. Геш функції.
16. Шифрування з автентифікацією.
17. Основні параметри блокових стандартів шифрування (DES, AES, ГОСТ 28147, ДСТУ 7624).
18. Основні параметри потокових стандартів шифрування (RC4, ДСТУ 8845).
19. Основні обчислення модулярної арифметики
20. Поняття і властивості алгебраїчних груп.
21. Важкі теоретико-числові проблеми.
22. Концепції шифрування з публічним ключем.
23. Розподіл ключів та шифрування з публічним ключем.
24. Алгоритми шифрування з публічним ключем.
25. Алгоритми цифрових підписів.
26. Схеми ідентифікації
27. Інфраструктура відкритих ключів.
28. Поняття криптопротоколів.
29. Криптопротоколи розподілу ключів.
30. Криптопротоколи автентифікації сторін.
31. Протоколи захисту мережевого трафіку IPSec.
32. Протоколи безпечної передачі даних прикладного рівня https.
33. Модель стеганосистеми.
34. Основні вимоги до стеганосистеми.
35. Відкриті, напівзакриті, закриті стеганосистеми.
36. Поняття ЦВЗ, класифікація.
37. Метод модифікації найменшого значущого біта.
38. Атаки на стеганосистеми.

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. Дистанційний курс University of Maryland by Jonathan Katz "Криптографія". https://www.coursera.org/course/cryptography.
2. Остапов С.Е. Технології захисту інформації : навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
3. Кузнецов О.О. Стеганографія : навчальний посібник / О.О. Кузнецов, С.П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.

ДОДАТКОВА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. Henk C.A. van Tilborg, FUNDAMENTALS OF CRYPTOLOGY. A Professional Reference and Interactive Tutorial. Eindhoven University of Technology. The Netherlands. KLUWER ACADEMIC PUBLISHERS, Boston/Dordrecht/London.
2. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих.

Інформаційні ресурси в Інтернеті:

1. https://www.coursera.org/course/cryptography
2. https://www.coursera.org/course/crypto
3. https://www.coursera.org/course/crypto2
4. https://www.cryptool.org/en/