

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

Кафедра кібербезпеки та DATA-технологій факультету №6

РОБОЧА ПРОГРАМА

навчальної дисципліни "Прикладна криптологія"

обов'язкових компонент

освітньої програми першого рівня вищої освіти

"Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем)"

Харків 2023

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол № 7 від 30.08.2023

СХВАЛЕНО

Вченою радою факультету №6
Протокол № 7 від 25.08.2023

ПОГОДЖЕНО

Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол № 7 від 29.08.2023

Розглянуто на засіданні кафедри кібербезпеки та DATA–технологій факультету №6
(протокол №8 від 15.08.2023)

Розробник: професор кафедри протидії кібербезпеки та DATA–технологій
факультету, к.т.н. доцент Носов В.В.

Рецензенти:

доцент кафедри кібербезпеки та DATA-технологій факультету №6 Харківського
національного університету внутрішніх справ к.т.н. доцент Тулупов В.В.

завідувач кафедри інформаційних управляючих систем Харківського національного
університету радіоелектроніки, д.т.н. професор Петров К.Е.

1. Мета та завдання навчальної дисципліни

Мета: ознайомлення з теоретичними основами криптографії та стеганографії, прикладними аспектами їх застосування.

Завдання:

- закладання основ знань та умінь використання криптографічних і стеганографічних систем;
- формування навичок аналізу та застосування криптографічних систем і протоколів при забезпеченні кібербезпеки.

Міждисциплінарні зв'язки: спирається на Вищу математику, Основи кібербезпеки, Інформаційні та комунікаційні технології, Теорію інформації та кодування; забезпечує Управління та організація систем захисту інформації, Цифрова криміналістика.

Очікувані результати навчання:

знати: концепції шифрування з секретним ключем; теоретичні основи досконалої і обчислювальної секретності; доказовість безпечності криптографії; методи автентифікації повідомлень; концепції шифрування з публічним ключем; цифрові підписи; криптографічні протоколи; основні поняття цифрової стеганографії;

вміти: здійснювати криптографічний аналіз криптограм класичних шифрів; дотримуватися умов безпеки криптосистем з секретним ключем; реалізовувати окремі операції шифрів симетричної і асиметричної криптографії, функції гешування в пакетах математичного моделювання; застосовувати програмні реалізації алгоритмів симетричної і асиметричної криптографії, електронного цифрового підпису; аналізувати криптографічні протоколи; проводити тестові атаки на ключову інформацію реалізованих криптографічних алгоритмів.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов	
Загальні компетентності (ЗК)	ЗК 1	Здатність застосовувати знання у практичних ситуаціях.
	ЗК 2	Знання та розуміння предметної області та розуміння професії.
	ЗК 4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням
Фахові компетентності спеціальності (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.

	КФ 10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності
--	-------	---

2. Програма навчальної дисципліни

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 поточкових (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.

3. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни				Вид контр олю
	Всьо го	з них:			
		лекц ії	Лабора торні занят тя	Сам остій на робо та	
Семестр №5					
Тема №1. Криптосистеми з секретним ключем	120	26	24	70	залік
Всього за семестр №5	120	26	24	70	
Семестр №6					
Тема №1. Криптосистеми з секретним ключем	18	4	6	8	екз.
Тема №2. Криптосистеми з публічним ключем	66	20	20	26	
Тема №3. Криптографічні протоколи	18	4	6	8	
Тема № 4. Цифрова стеганографія	18	6	4	8	
Всього за семестр №6	120	34	36	50	
Всього за дисципліною	240	60	60	120	

4.1.2. Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни				Вид контр оліо
	Всьо го	з них:			
		лекц ії	Лабора торні занят тя	Сам остій на робо та	
Семестр №5					
Тема №1. Криптосистеми з секретним ключем	120	4	8	108	залік
Всього за семестр №5	120	4	8	108	
Семестр №6					
Тема №2. Криптосистеми з публічним ключем	72	2	4	66	екз.
Тема №3. Криптографічні протоколи	24	1	2	21	
Тема № 4. Цифрова стеганографія	24	1	2	21	
Всього за семестр №6	120	4	8	108	
Всього за дисципліною	240	8	16	228	

4.1.2. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни		Література
Тема №1. Криптосистеми з секретним ключем		
1. Розрахунок безумовних ймовірностей букв українського алфавіту за довільним текстовим фрагментом.	3,5,6,8	
2. Програмна реалізація нижченаведених шифрів:		
1) Цезаря;		
2) простої заміни;		
3) Віженера;		
4) Вернема;		
5) Плейфера;		
6) перестановок.		
3. Програмна реалізація криптографічного аналізу криптограм шифру простої заміни.		
4. Програмна реалізація алгоритм генерації псевдовипадкової послідовності.		
Тема №2. Криптосистеми з публічним ключем		
1. Програмна реалізація нижченаведених алгоритмів:	3,5,6,8,9	
1) Diffie-Hellman;		
2) Elgamal;		
3) RSA;		
4) Elliptic curve.		
Тема №3. Криптографічні протоколи		
1. Криптографічні протоколи, що вже реалізовані на практиці.	Ресурси Internet	
2. Перспективні протоколи квантової криптографії.		
Тема №4. Цифрова стеганографія		
1. Метод модифікації найменшого значущого біта.	5, Ресурси Internet	
2. Атаки на стеганосистеми		

4. Індивідуальні навчально-дослідні завдання

5.1.1. Теми рефератів

1. Проблеми і задачі сучасної криптографії.
2. Принципи та технології побудови криптографічних алгоритмів.
3. Оптимізація криптографічних параметрів вузлів і блоків шифраторів.
4. Синтез криптографічних шифрів.
5. Організація мереж засекреченого зв'язку.
6. Сучасні принципи та технології ключових систем криптографії.
7. Перспективні криптографічні протоколи.
8. Формальний аналіз криптографічних протоколів.
9. Програмні інструменти атаки на криптографічні ключі.

5. Методи навчання

Аудиторні заняття проводяться у формі візуального представлення аналітично-графічного матеріалу дисципліни, на яких курсанти повинні виконувати відповідні розумові, обчислювальні та практичні дії.

Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять, опрацювання завдань лабораторних занять.

Індивідуальна робота передбачає написання рефератів.

6. Перелік питань та завдань, 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 поточкових 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.

7. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних і лабораторних занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та лабораторних занять і має за мету перевірку засвоєння знань, умінь і навичок здобувачем вищої освіти (далі – здобувач) з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів враховуються такі види робіт: навчальні заняття (практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт 10.

$$\begin{array}{l} \text{Загальна кількість} \\ \text{балів} \\ \text{підсумковим} \\ \text{контролем) } \end{array} \quad \begin{array}{l} \text{Результат} \\ \text{навчальних} \\ \text{занять} \\ \text{за семестр} \end{array} \quad = \left(\begin{array}{l} \text{Результат} \\ \text{самостійної} \\ \text{роботи за} \\ \text{семестр} \end{array} \right) \cdot \frac{2}{1} \cdot 10$$

Підсумковий контроль. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструється в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображаються у відомостях обліку успішності, навчальних картках здобувачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то

науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переведення результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50**.

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені, заліку).

$$\text{Підсумкові бали навчальної дисципліни} = \frac{\text{Загальна кількість балів (перед підсумковим контролем)}}{\text{Кількість балів за підсумковим контролем}}$$

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

$$\frac{\text{Підсумкові бали навчальної дисципліни}}{\text{Підсумкові бали за поточний семестр}} = \frac{\text{Підсумкові бали за попередній семестр}}{2}$$

Критерії оцінювання здобувачів вищої освіти під час поточного контролю (робота на практичних, лабораторних заняттях, самостійна робота, виконання індивідуальних творчих завдань) та підсумкового контролю.

Робота під час навчальних занять	Самостійна та індивідуальна робота	Підсумковий контроль
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати звіт за темою самостійної роботи.	Отримати за підсумковий контроль не менше 30 балів

8. 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			
70 –74	Задовільно ("зараховано")	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.
65-69			
60–64			
41–59	Незадовільно ("не зараховано")	D	"Задовільно" – теоретичний зміст курсу освоєний не повністю , але прогалини не несуть 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.
21-40			
1–20			
41–59	Незадовільно ("не зараховано")	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.
21-40			
1–20			
41–59	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			
41–59	Незадовільно ("не зараховано")	F	"Безумовно незадовільно" – теоретичний зміст курсу не освоєно , необхідні практичні навички роботи не
21-40			
1–20			

Оцінка в балах	Оцінка за національно ю шкалою	Оцінка за шкалою ECTS	
		Оцін ка	Пояснення
			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

9. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна

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. Євсєєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
3. Кузнецов О.О. Стеганографія : навчальний посібник / О.О. Кузнецов, С.П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.

Додаткова

4. 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.
5. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих.

Інформаційні ресурси

6. <https://www.coursera.org/course/cryptography>
7. <https://www.coursera.org/course/crypto>
8. <https://www.coursera.org/course/crypto2>
9. <https://www.cryptool.org/en/>