Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Голова НМК
_____ Д.М. Крицький
(підпис) (ініціали та прізвище)

« 31 » 08 2021 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи побудови та аналізу криптосистем
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

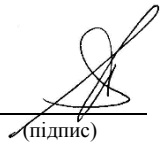
Рівень вищої освіти: другий (магістерський)

Харків 2021 рік

Розробник: Олійников Р.В., професор, д.т.н., доц. 
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від «30» 08 2021р.

Завідувач кафедри д.т.н., професор  В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни
(денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 4</td><td rowspan="11">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних і комунікаційних систем
(найменування)

Рівень вищої освіти:
другий (магістерський)</td><td>Вибіркова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 6</td><td>2021/2022</td></tr>
<tr><td>Індивідуальне завдання:
немає
(назва)</td><td>Семестр</td></tr>
<tr><td>Загальна кількість годин – 40 / 80</td><td>2-й</td></tr>
<tr><td rowspan="7">Кількість тижневих годин для денної форми навчання:
аудиторних – 3/3
самостійної роботи студента – 3/3</td><td>Лекції *</td></tr>
<tr><td>32 годин</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>8 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>80 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: 40/125.

*Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: засвоєння принципів побудування, аналізу властивостей та реалізації симетричних та асиметричних криптографічних алгоритмів, а також атак на них.

Завдання:

– вивчити основні поняття криптографічного захисту інформації;

– вивчити принципи побудування криптографічних примітивів та типи атак на них;

– вивчити принципи функціонування інфраструктури відкритих ключів;

– вивчити вимоги до симетричних блокових шифрів, принципи їх побудування та сутність диференційного криптоаналізу;

– вивчити особливості побудування та ефективної програмної реалізації блокового шифру AES;

– вивчити принципи побудування потокових шифрів та інших симетричних примітивів;

– вивчити принципи побудування алгоритмів з відкритим ключем та атак на них.

Компетентності, які набуваються.

–Знання та розуміння предметної області та розуміння професії.

–Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

–Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

–Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

–Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

Очікувані результати навчання:

– організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

– використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

– аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

– адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

– критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
– впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
– вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
– застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
– вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
– застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
– вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
– виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

Пререквізити - вивчення дисципліни на знанні дисциплін «Вища математика», «Дискретна математики», «Прикладна криптологія» та «Апаратні та програмні засоби захисту інформації».

Знання, вміння і навики, придбані при вивченні дисципліни необхідні як при теоретичних дослідженнях у галузі криптографічної інформації, так і при практичної діяльності при побудові, експертизі та застосуванні сучасних систем захисту інформації із криптографічною підсистемою.

Кореквізити –"Дипломний проект (робота) бакалавра".

3. Програма навчальної дисципліни

Модуль 1. Теорія криптографічних примітивів, принципи побудування та криптоаналізу симетричних блокових шифрів. Принципи побудування та ефективної реалізації блокових шифрів, потокові шифри та алгоритми з відкритим ключем.

Змістовний модуль 1. Введення у криптографію.

Тема 1. Сучасні атаки на програмне забезпечення.

Атаки на програмне забезпечення смартфонів, Smart TV та ін. та застосування криптографії для його захисту.

Тема 2. Етапи розвитку криптографії.

Шифри перестановки та підстановки. Поліалфавітна перестановка. Сучасна криптографія.

Тема 3. Основні поняття захисту інформації.

Основні властивості інформації. Основні визначення криптографічних послуг безпеки. Математичні методи сучасної інформаційної безпеки. Принцип Керкгоффса.

Модульний контроль.

Змістовний модуль 2. Криптографічні примітиви та атаки на них.

Тема 1. Криптографічні примітиви.

Основні визначення щодо шифрування. Типи шифрування. Симетричне шифрування. Блоковий та потоковий шифри. Зашифрування з відкритим ключем. Атака «зустріч посередині». Цифровий підпис. Геш-функція. Застосування цифрового підпису. Криптографічний протокол. Криптографія на основі ідентифікаторів.

Тема 2. Інфраструктура відкритих ключів.

Центр сертифікації ключів. Кореневий центр сертифікації. Крос-сертифікація. Сертифікат X.509 v3. Список відкликаних сертифікатів. Причини відкликання сертифікату. Протокол OCSP (Online Certificate Status Protocol).

Тема 3. Криптоаналітичні атаки та класи стійкості шифрів.

Класи криптоаналітичних атак. Атаки на схеми зашифрування. Моделі оцінки безпеки. Типи атак на алгоритми шифрування. Атака вичерпного пошуку та словникова атака. Атака на основі застосування таблиць передобчислень. Ідеальний шифр, принципи побудування та властивості. Безумовно стійкі та практично (обчислювально) стійкі шифри.

Модульний контроль.

Змістовний модуль 3. Симетричні блокові шифри та диференційний криптоаналіз.

Тема 1. Симетричний блоковий шифр DES.

Принципи побудування блокового шифру DES. Циклова функція симетричного блокового шифру DES. Ефективна програмна реалізація симетричного блокового шифру DES.

Тема 2. Вимоги до симетричних блокових шифрів.

Вимоги та принципи побудування симетричних блокових шифрів. Лавинний ефект для блокових шифрів та геш-функцій.

Тема 3. Диференційний (різницевий) криптоаналіз.

Сутність диференційного криптоаналізу. Диференційні властивості підстановки блокового шифру DES. Механізм відновлення бітів ключа при знанні вхідних різниць підстановки. Операція додавання ключа. Різниці у цикловій функції блокового шифру DES. Складність диференційного криптоаналізу блокового шифру DES.

Тема 4. Послідовники блокового шифру DES.

Блоковий шифр Triple DES. Стійкість та властивості реалізації блокового шифру Triple DES. Блоковий шифр Skipjack.

Модульний контроль.

Змістовний модуль 4. Симетричний блоковий шифр AES та режими роботи симетричного блокового шифру.

Тема 1. Симетричний блоковий шифр AES.

Властивості блокового шифру AES. Математичні принципи побудування блокового шифру AES. Параметри блокового шифру AES. Високорівнева структура блокового шифру AES. Основні перетворення циклової функції блокового шифру AES. Схема розгортання ключів блокового шифру AES. Алгоритм розшифрування блокового шифру AES.

Тема 2. Програмна реалізація блокового шифру AES.

Принципи ефективної програмної реалізації блокового шифру AES. Оптимізація алгоритму розшифрування блокового шифру AES. Рекомендації щодо програмної реалізації блокового шифру AES.

Тема 3. Режими роботи симетричного блокового шифру.

Режим електронної кодової книги та його переваги й недоліки. Режим зчеплення блоків шифртексту та його переваги й недоліки. Режим зворотного зв'язку по шифртексту та його переваги й недоліки. Режим зворотного зв'язку по виходу та його переваги й недоліки. Режим лічильника та його переваги й недоліки. Додаткові режими блокового шифру. Рекомендації щодо реалізації режимів блокового шифру.

Модульний контроль.

Змістовний модуль 5. Потокові шифри та інші симетричні примітиви.

Тема 1. Потокові шифри.

Потоковий шифр A5/1. Регістр зсуву з лінійним зворотним зв'язком. Ефективна програмна реалізація шифрів, заснованих на регістрі зсуву з лінійним зворотним зв'язком. Сучасні потокові шифри. Потоковий шифр SNOW. Потоковий шифр ZUC.

Тема 2. Інші симетричні примітиви.

Малоресурсна криптографія. Блоковий шифр PRESENT. Генератори псевдовипадкових послідовностей засновані на блокових шифрах.

Модульний контроль.

Змістовний модуль 6. Криптографія з відкритим ключем та загальні вразливості криптографічних алгоритмів.

Тема 1. Математичні основи криптографії з відкритим ключем.

Прості числа. Функція Ейлера. Відношення конгруентності та клас конгруентності. Теорема Ейлера.

Тема 2. Алгоритми з відкритим ключем.

Протокол обміну ключами Діффі-Геллмана. Алгоритм RSA. Генерація пари ключів для алгоритму RSA. Зашифрування та розшифрування за алгоритмом RSA. Сучасні алгоритми з відкритим ключем. Комбінація симетричного алгоритму з алгоритмом з відкритим ключем. Рекомендовані довжини ключів для алгоритмів з відкритим ключем.

Тема 3. Вразливості криптографічних алгоритмів.

Атаки по стороннім каналам. Криптографічні вразливості: недостатній аналіз розробленого алгоритму, застосування застарілих перетворень та некоректне застосування перетворень. Атака розширення довжини на конструкцію Меркля-Дамгарда. Застосування слабкого протоколу управління ключами. Рекомендації щодо застосування криптографічних алгоритмів.

Модульний контроль.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1. Введення у криптографію.					
Тема 1. Сучасні атаки на програмне забезпечення.	3	1			2
Тема 2. Етапи розвитку криптографії.	3	1			2
Тема 3. Основні поняття захисту інформації. Модульний контроль.	7	2			5
Разом за змістовим модулем 1	13	4			9
Змістовий модуль 2. Криптографічні примітиви та атаки на них.					
Тема 1. Криптографічні примітиви.	9	2		2	5
Тема 2. Інфраструктура відкритих ключів.	7	2			5
Тема 3. Криптоаналітичні атаки та класи стійкості шифрів. Модульний контроль.	7	2			5
Разом за змістовим модулем 2	23	6		2	15
Змістовий модуль 3. Симетричні блокові шифри та диференційний криптоаналіз.					
Тема 1. Симетричний блоковий шифр DES.	7	1		2	4
Тема 2. Вимоги до симетричних блокових шифрів.	5	1			4
Тема 3. Диференційний (різницевий криптоаналіз).	6	2			4
Тема 4. Послідовники блокового шифру DES. Модульний контроль.	6	2			4
Разом за змістовим модулем 3	24	6		2	16
Усього годин	60	16		4	40
Змістовий модуль 4. Симетричний блоковий шифр AES та режими роботи симетричного блокового шифру.					
Тема 1. Симетричний блоковий шифр AES.	8	2			6
Тема 2. Програмна реалізація блокового шифру AES.	10	2		2	6
Тема 3. Режими роботи симетричного блокового шифру. Модульний контроль.	10	2		2	6
Разом за змістовим модулем 1	28	6		4	18
Змістовий модуль 5. Потокові шифри та інші симетричні примітиви.					
Тема 1. Потокові шифри.	7	2			5
Тема 2. Інші симетричні примітиви. Модульний контроль.	7	2			5
Разом за змістовим модулем 2	14	4			10

1	2	3	4	5	6
Змістовий модуль 6. Криптографія з відкритим ключем та загальні вразливості криптографічних алгоритмів.					
Тема 1. Математичні основи криптографії з відкритим ключем.	6	2			4
Тема 2. Алгоритми з відкритим ключем.	6	2			4
Тема 3. Вразливості криптографічних алгоритмів	6	2			4
Разом за змістовим модулем 3	18	6			12
Усього годин	120	32		8	80

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	
	Разом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Інтерфейс командного рядка криптографічної бібліотеки OpenSSL	2
2	Інтерфейс мови програмування с криптографічної бібліотеки OpenSSL	2
3	Ефективна реалізація симетричного блокового шифру AES	2
4	Основні режими роботи блокового шифру та атаки на них	2
	Разом	**8**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Вивчення основних понять криптографічного захисту інформації.	9

2	Вивчення загальних принципів побудування криптографічних примітивів та типів атак на них.	15
3	Вивчення принципів побудування симетричних примітивів та диференційного криптоаналізу.	16
4	Вивчення особливостей блокового шифру AES.	18
5	Вивчення принципів побудування потокових шифрів.	10
6	Вивчення принципів побудування алгоритмів з відкритим ключем та атак на них.	12
	Разом	**80**

9. Індивідуальні завдання

Не передбачено

10. Методи навчання

Проведення аудиторних лекцій, практичних, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, модульного контролю, підсумковий контроль у вигляді екзамену.

12. Критерії оцінювання та розподіл балів, які отримують студенти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модульний контроль			
Теми 1-3			
Робота на лекціях	0…1	6	0…6
Виконання і захист лабораторних робіт	3...5	4	12...20
Модульний контроль	18…22	1	18…22
Теми 4-6			
Робота на лекціях	0…1	8	0…8
Виконання і захист лабораторних робіт	3...5	4	12...20
Модульний контроль	18…24	1	18…24
Усього за семестр			**60…100**

Семестровий контроль у вигляді заліку проводиться у разі відмови студента від балів поточного тестування. Під час складання семестрового заліку студент має можливість отримати максимум 100 балів.

Білет для іспиту/заліку складається з визначення криптосистеми (до 20 балів), вимог до крос-сертифікації (до 30 балів), режиму роботи CTR блокового шифра (до 20 балів), прикладу генерації ключової пари RSA для заданих невеликих простих чисел (до 30 балів).

Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

- знати базові поняття криптографічного захисту інформації;
- знати основні методи симетричних і асиметричних криптографічних перетворень;
- знати базові методи криптоаналізу.

Необхідний обсяг вмінь для одержання позитивної оцінки:
- уміти використовувати сучасний інструментарій у вигляді бібліотеки OpenSSL для вирішення задач базових криптографічних перетворень;
- уміти власно реалізувати симетричне криптографічне перетворення (шифр AES);
- уміти власно реалізувати режими роботи блокових шифрів;
- уміти продемонструвати роботу методів криптоаналізу для режимів роботи блокових шифрів.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань лабораторних занять. Вміти самостійно давати характеристику існуючої криптосистеми, проводити оцінку її стійкості. Вміти обґрунтувати основні показники обраної криптосистеми.

Добре (75-89). Твердо знати мінімум, захистити не менше 90% завдань лабораторних занять. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах. Вміти пояснювати способи обґрунтування стійкості та виконувати аналіз окремих компонентів криптосистеми, що мають критичний вплив на загальну стійкість.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Орієнтуватися у підручниках та посібниках. Досконально знать усі технології, які використовуються при проектуванні сучасних криптосистем. Вміти будувати складні системи на основі стандартних компонентів, визначених національними і міжнародними стандартами, виконувати аналіз їхньої стійкості та загальної ефективності. Безпомилково виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

1. Олійников Р.В. Слайди (конспект) лекцій.
2. Олійников Р.В. Лабораторні роботи.
3. Олійников Р.В. Методичні вказівки щодо виконання лабораторних робот.

14. Рекомендована література

Базова література

1. За редакцією Горбенко І.Д. Горбенко Ю.І. «Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації». Монографія. Харків. Форт. 2015 , 902с.
2. За редакцією Горбенко І.Д. Горбенко Ю.І. «Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації». Електронна версія. Монографія. Харків. Форт. 2015 , 902с.
3. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. Монографія. Харків. Форт. 2010 , 593с.
4. Інфраструктура відкритих ключів: технології, архітектура, побудова та впровадження / [О. В. Потій, А. В. Лєншин, Л. С. Сорока, В. І. Єсін і ін.]. – Дніпропетровськ: Академія митної служби України, 2011. 202с.
5. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків. Форт. 2013р. , 878с.

Додаткова література

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: «Триумф», 2002. 797 с.
2. Венбо Мао. Современная криптография : теория и практика[Электронный ресурс] .— М. : Издательский дом Вильямс, под редакцией Клюшиной Д.А. .— 2005. 768 с. Режим доступа: https://search.rsl.ru/ru/record/01002724428.
3. Романьков В.А. Алгебраическая криптография [Электронный ресурс]: монография/ Романьков В.А.— Электрон. текстовые данные.— Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. 136 с.— Режим доступа: http://www.iprbookshop.ru/24868.html.— ЭБС «IPRbooks»
4. E. Biham, N. Keller. Cryptanalysis of Reduced Variant of Rijndae. [Електронний ресурс]. –Режим доступу: http://cscr. nist. gov/encryption/aes/round2/conf3/aes3papers. html
5. Шеннон К. Работы по теории информации и кибернетике. – М.: ИЛ, 1963. 830 с. (Раздел – Теория связи в секретных системах).
6. Шнайер Б. Безопасность данных в цифровом мире. – СПб: Питер, 2003. 367 с.

7. 8.Ю. Юдін О.К, Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К. Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. 716 с.

8. Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 2010.

9. Viega, John, Matt Messier, and Pravir Chandra. Network Security with OpenSSL: Cryptography for Secure Communications. O'Reilly, 2009.

10. ДСТУ ITU-TRec.X.509 | ISO/IEC 9594-8:2006 «Інформаційнітехнології. Взаємозв'язок відкритих систем.Каталог:Основні положення щодо сертифікації відкритих ключів та сертифікації атрибутів».