Опис програми кредитного модуля

ВП-02 «Засоби захисту інформації»
(код та назва кредитного модуля, дисципліни)

Статус кредитного модуля _____
(обов'язкова або за вільним вибором студентів)

Лектор Артеменко Віктор Андрійович, доцент
(прізвище, ім'я та по батькові, посада)

Інститут/факультет Теплоенергетичний
(назва)

Кафедра АПЕПС
(назва)

І. Загальні відомості

Курс "Засоби захисту інформації" належить до циклу дисциплін з Інформаційних технологій проектування і Програмного забезпечення автоматизованих систем і охоплює: моделі загроз інформації, механізми та сервіси її захисту, криптографічні методи забезпечення її конфіденційності, цілісності та нон-репудіації (унеможливлення відмови від виконаних дій, або обов'язків, що були прийняті), аутентифікації суб'єктів та об'єктів інформаційної діяльності.

Цей курс базується на таких забезпечуючих дисциплінах: «Вища математика», «Спецрозділи математики», «Теорія ймовірностей та математична статистика», «Алгоритмічне програмування», «Об'єктно-орієнтоване програмування», «Теорія інформації та кодування», «Основи теорії інформаційних процесів».

Обсяг у кредитах ECTS: 3 кредити.

ІІ. Розподіл навчального часу

Семестр	Код кредит. модуля	Всього (кред./год)	Розподіл за видами занять (всього год./год. у тижні)			СРС	Модульні контрольні роботи (кільк.)	Індивід. завдання (вид)	Вид семестр. атестац.
			Лекції	Практичні/ семінарські	Лабораторні/ комп'ют. практикум				
10	ВП-02	3/108	18	-	18	72	1		залік/д

ІІІ. Мета і завдання кредитного модуля

Цей курс забезпечує та поглиблює засвоєння студентами наступних дисциплін: «Цифрова обробка сигналів та зображень», «Операційні системи», «Системи управління базами даних», «Системи та мережі передачі даних», «Комп'ютерні мережі», «Програмно апаратні засоби бездротового зв'язку», «Телекомунікаційні системи та мережі», «Управління в телекомунікаційних мережах», «Надійність та безпека інформаційних та інформаційно-управляючих систем та мереж», «Способи та засоби підвищення ефективності передачі та обробки інформації».

Дисципліна включає в себе систему змістовних модулів відповідно до стандарту СВО ОПП Бакалавр, напряму підготовки 6.050101 Комп'ютерні науки, з узагальненим об'єктом діяльності - комп'ютерні інформаційні системи і технології. Система змістовних модулів СВО наведена у таблиці нижче.

Витяг з Додатку Б - Система змістовних модулів СВО

Зміст уміння, що забезпечується	Шифр уміння	Назва змістовного модуля	Шифр змістовного модуля
1.	2.	3.	4.
Забезпечувати надійне функціонування системного програмного забезпечення в умовах експлуатації прикладного програмного забезпечення за допомогою сучасних діагностичних засобів, використовуючи системи захисту технічних і програмних засобів від несанкціонованого доступу.	ПФ.Д.01.ПР.Р.02	Процедури та алгоритми забезпечення захисту прог-рамних систем від несанк-ціонованого доступу.	ПФ.Д.01.ПР.Р.02.01
		Апаратні засоби захисту інформації.	ПФ.Д.01.ПР.Р.02.02
Розробляти програмні *засоби* та організаційні заходи щодо *захисту баз даних* від несанкціонованого доступу в екстремальних умовах (локальні і глобальні комп'ютерні мережі, багаточисельний склад користувачів) за допомогою сучасних програмних і технічних засобів, використовуючи фізичні методи захисту, персональну ідентифікацію користувачів, шифратори в комп'ютерній мережі тощо.	ПФ.Д.02.ПП.Р.01	Авторизація доступу до даних, захист даних від несанкціонованого доступу.	ПФ.Д.02.ПП.Р.01.01
		Методи забезпечення цілісності, конфіденційності даних	ПФ.Д.02.ПП.Р.01.02
Контролювати та відновлювати *цілісність даних* у базах даних в умовах експлуатації баз даних і прикладних програм за допомогою програмно-технічних засобів та тестів, використовуючи резервне копіювання, захист даних від несанкціонованого доступу, секретність даних.	ПФ.Д.07.ПП.Р.01	Забезпечення, контроль та відновлення цілісності даних в базах даних.	ПФ.Д.07.ПП.Р.01.01
Забезпечувати захист даних в мережах в умовах несанкціонованого доступу за допомогою спеціальних програмних і технічних засобів, використовуючи процедури	ПФ.Д.04.ПП.Р.02	Методи та засоби захисту інформації в комп'ютерних мережах .	ПФ.Д.04.ПП.Р.02.01

використовуючи процедури дистанційної реєстрації подій, резервування даних на сервері, перевірки захищеності комп'ютера і паролів, контроль змін в системних файлах, систему аутентифікації тощо.		Організаційні, правові, фізичні методи та заходи захисту інформації в комп'ютерних мережах.	ПФ.Д.04.ПП.Р.02.02

Система блоків змістовних модулів стандарту СВО відповідного напряму, вивчення яких забезпечується даною дисципліною наведена у наступній таблиці

Витяг з Додатку В - Система блоків змістовних модулів стандарту СВО

Шифр блоку змістовних модулів	Назви блоків змістовних модулів	Назви змістовних модулів, що входять до даного блоку	Шифри змістовних модулів
1.	2.	3.	4.
ПП.63	Принципи побудови систем та засобів захисту програмного забезпечення.	Процедури та алгоритми забезпечення захисту програмних систем від несанкціонованого доступу.	ПФ.Д.01.ПР.Р.02.01
		Апаратні засоби захисту інформації.	ПФ.Д.01.ПР.Р.02.02
ПП.65	Методи та засоби захисту програмного забезпечення та даних.	Авторизація доступу до даних, захист даних від несанкціонованого доступу.	ПФ.Д.02.ПП.Р.01.01
		Методи забезпечення цілісності, конфіденційності даних	ПФ.Д.02.ПП.Р.01.02
		Забезпечення, контроль та відновлення цілісності даних в базах даних.	ПФ.Д.07.ПП.Р.01.01
ПП.69	Захист інформації в комп'ютерних мережах.	Методи та засоби захисту інформації в комп'ютерних мережах .	ПФ.Д.04.ПП.Р.02.01
		Організаційні, правові, фізичні методи та заходи захисту інформації в комп'ютерних мережах	ПФ.Д.04.ПП.Р.02.02

В результаті вивчення дисципліни студенти повинні

ЗНАТИ:

- Моделі загроз інформації.
- Моделі зловмисників та порушників інформаційної безпеки.
- Механізми захисту інформації.
- Головні задачі та сервіси захисту інформації.

- Традиційні (моноключові, симетричні) класичні криптосистеми: Цезаря, Тритеміуса, Гамірування, Віжинера, з перестановками символів повідомлення, з перестановками символів алфавіту, тощо.
- Традиційні (моноключові, симетричні) сучасні криптосистеми: DES, 3DES, Blowfish, Twofish, ГОСТ 28147 – 89, AES, тощо.
- Математичні засади криптографічних перетворень інформації.
- Теорію чисел, властивості простих чисел.
- Проблему факторизації числа.
- Теореми Ферма, Мебіуса, Ейлера.
- Арифметичні системи з обмеженим алфавітом. Скінченні поля Галуа GF(p).
- Мультиплікативне обернення елементів поля Галуа GF(p).
- Алгоритм Евкліда, розширений алгоритм Евкліда.
- Дискретне піднесення числа до степеня.
- Проблему дискретного логарифмування.
- Проблему розподілу моноключа в традиційних криптосистемах. Алгоритм Diffie - Hellman.
- Асиметричні криптосистеми (двоключові, з відкритим ключем): RSA, El Gamal.
- Проблема співвідношення: актуальність інформації – криптостійкість захисту – витрати на захист інформації.
- Односторонні функціональні перетворення. Hash-функції. Колізії у Hash-функції.
- Електронний цифровий підпис. Алгоритми ЕЦП. Приклади стандартів ЕЦП: DSS, ЕЦП на еліптичних кривих.
- Інфраструктура відкритих ключів. Сертифікати відкритих ключів X.509.
- Складні процедури та міжнародні протоколи криптографічного захисту інформації.
- Протоколи автентифікації (Kerberos, TACACS, RADIUS та ін.).
- Захист інформації в комп'ютерних мережах.

ВМІТИ:

- Аналізувати та виявляти загрози інформації.
- Розробляти моделі зловмисників та порушників інформаційної безпеки.
- Обґрунтовано обирати механізми захисту інформації.
- Добирати сервіси відповідно головним задачам захисту інформації.
- Кодувати та декодувати повідомлення симетричними шифрами: Цезаря, Тритеміуса, Гамірування, Віжинера, з перестановками символів повідомлення, з перестановками символів алфавіту.
- Кодувати та декодувати повідомлення сучасними симетричними шифрами: DES, 3DES, Blowfish, Twofish, AES, ГОСТ 28147 – 89, тощо.
- Виконувати з криптографічною метою математичні перетворення над елементами даних, що несуть інформацію (обмежені алфавіти).

- Перевірити чи є число простим, побудувати просте число (обернене завдання).
- Розкладати числа на прості множники (проблемне завдання).
- Застосовувати Теореми Ферма, Мебіуса, Ейлера у криптографічних перетвореннях та побудовах.
- Виконувати арифметичні та алгебраїчні операції над скінченними полями Галуа GF(p).
- Виконувати мультиплікативне обернення елементів поля Галуа GF(p).
- Виконувати алгоритм Евкліда, розширений алгоритм Евкліда.
- Виконувати дискретне піднесення числа до степеня.
- Будувати та використовувати циклічну структуру адитивної та мультиплікативної груп GF(p) скінченого поля Галуа (певний аналог добування кореня).
- Виконувати розподіл моноключа за алгоритмом Diffie - Hellman.
- Кодувати та декодувати повідомлення асиметричними шифрами: RSA, El Gamal.
- Аналізувати співвідношення: актуальність інформації – криптостійкість захисту – витрати на захист інформації.
- Організовувати виконання обчислення Hash-функції за алгоритмом MD5.
- Організовувати виконання обчислення ЕЦП за алгоритмом El Gamal.
- Організовувати виконання обчислення ЕЦП на еліптичних кривих.
- Організовувати інфраструктуру сертифікатів відкритих ключів за рекомендацією X.509.
- Організовувати використання складних криптографічних процедур за міжнародними протоколами криптографічного захисту інформації.
- Використовувати міжнародні протоколи автентифікації (Kerberos, TACACS, RADIUS та ін.).
- Організовувати захист інформації в комп'ютерних мережах.

IV. Зміст кредитного модуля

Кредитний модуль : Засоби захисту інформації

Розділ 1 **Загрози інформації. Механізми та сервіси її захисту.**

Тема 1.1 Модель загроз інформації. Механізми та сервіси її захисту.

Тема 1.2 Класифікація атак на інформацію та інформаційну систему. Моделі порушень інформаційної безпеки. Моделі зловмисника.

Розділ 2 **Традиційні криптосистеми. Симетричні шифри.**

Тема 2.1 Модель симетричної криптосистеми.

Тема 2.2 Традиційні криптосистеми. Ретроспектива.

Тема 2.3 Традиційні криптосистеми. Сучасні методи. Криптосистема DES.

Тема 2.4 Сучасні симетричні криптосистеми (ГОСТ 28147-89, AES, xDES).

Розділ 3 Математичні засади криптографічних перетворень інформації.

Тема 3.1 Теорія чисел, властивості простих чисел.

Тема 3.2 Теореми Ферма, Мебіуса, Ейлера. Проблема факторизації числа.

Тема 3.3 Скінченні поля Галуа. Арифметичні системи з обмеженим алфавітом.

Тема 3.4 Мультиплікативне обернення елементів поля Галуа GF(p).

Тема 3.5 Алгоритм Евкліда, розширений алгоритм Евкліда.

Тема 3.6 Дискретне піднесення числа до степеня. Проблема дискретного логарифмування.

Розділ 4 Криптографія з відкритим ключем. Асиметричні шифри.

Тема 4.1 Модель асиметричної криптосистеми.

Тема 4.2 Криптосистема Diffie - Hellman.

Тема 4.3 Криптосистема RSA.

Тема 4.4 Криптосистема El Gamal.

Тема 4.5 Електронний цифровий підпис (ЕЦП).

V. Методи навчання та інформаційно-методичне забезпечення

При вивченні тем Розділу 1 потрібно звернути увагу студентів на те, що модель зловмисника витікає з моделі порушень інформаційної безпеки, яка, у свою чергу, витікає з моделі загроз інформації. На питання, яким чином виконувати захист інформації у системі, відповідають механізми захисту. А реалізація тих механізмів в інформаційних системах надає нам сервіси захисту інформації.

При вивченні тем Розділу 2 потрібно підкреслити важливе значення моделі симетричної (моноключової) криптосистеми, з огляду на те, що від найдавніших часів і до 1976 року це була єдина модель криптосистеми, взагалі відома людству. Необхідно, в рамках історичної ретроспективи, детально розібрати відомі традиційні симетричні класичні криптосистеми: Цезаря, Тритеміуса, Гамірування, Віжинера, з перестановками символів повідомлення, з перестановками символів алфавіту, із штучними алфавітами та ін., щоби засвоїти головну мотивацію їх розвинення та ускладнення – збільшення їх криптостійливості. Серед традиційних криптосистем особливу увагу слід приділити сучасним методам та їх яскравому представникові - криптосистемі DES, її подальшому розвиткові та вдосконаленню її методів у сучасних симетричних криптосистемах (ГОСТ 28147-89, xDES, IDEA, Blowfish, Twofish, RCx, CAST-128, AES). Мусимо звернути увагу студентів на логіку розвинення цих алгоритмів та механізми реалізації в них криптоперетворень.

При вивченні тем Розділу 3 потрібно мати на увазі важливе значення знань з теорії чисел, скінчених полів Галуа, алгоритмів Евкліда, невирішених

проблем дискретної математики (факторизації числа, дискретного логарифмування) для досконалого володіння методами сучасної криптографії.

В розділі 4 слід звернути увагу на Модель асиметричної криптосистеми, яка відкрито публікується з 1976 р. і розкриває найзагальніші особливості другої, серед існуючих, моделі криптосистем. Дуже важливо розуміти оберненість асиметричної криптосистеми, яку демонструє ця модель завдяки зміні функцій пари ключів. Саме ця оберненість дозволяє отримати у комплексі такі сервіси системи захисту, як конфіденційність, автентифікація, цілісність, неможливість відмови від виконаних у інформаційній системі дій. Спектр завдань, які вирішують асиметричні криптосистеми, простягається від розподілення ключів між користувачами до поставлення цифрового електронного підпису, і дозволяє взагалі зняти проблему потреби захищеного (секретного) каналу зв'язку у інформаційній системі.

Розділ 5 присвячений детальному вивченню висхідних ідей Діффі і Хеллмана про моно-направлені функціональні перетворення у криптографії та їх реалізації у відомих Хеш-алгоритмах. Потрібно чітко висвітити ті позиції, які вони займають у сучасній побудові захищених інформаційних систем, їх позитиви та недоліки, які визначають ці позиції.

Розділ 6 присвячений огляду процедур, міжнародних стандартів та протоколів автентифікації і криптографічного захисту інформації та вивченню найбільш розповсюджених з них. Потрібно звернути увагу студентів на накопичений світовий досвід з організації захисту інформації в комп'ютерних мережах та в прикладних програмах.

При вивченні питань Розділу 7 слід звернути увагу студентів на відомі шляхи порушення інформаційної безпеки в реальних системах та найбільш розповсюджених на поточний час порушників – комп'ютерні віруси. Серед засобів убезпечення від проникнення різних порушників в інформаційну систему одне з важливих місць займають Міжмережні екрани (firewalls), вивчення властивостей, функцій та налаштувань яких допоможе студентам у майбутньому використовувати їх для побудови захищених інформаційних систем.

Для забезпечення наочності навчальних занять, рекомендується використовувати проектор типу «Полілюкс» зі слайдами на прозорих плівках, або комп'ютер з проектором цифрових зображень та лекційними матеріалами, виконаними у вигляді презентацій у прикладні Power Point.

Основна література:

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Изд-во ТРИУМФ, 2002. - 816 с.: ил.
2. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил.
3. Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с.: ил.

Додаткова література:

1. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.: ил.
2. Анин Б.Ю. Защита компьютерной информации. - СПб.: БХВ-Санкт-Петербург, 2000. – 384 с.: ил.
3. Методи захисту фінансової інформації: Навчальний посібник / В.К. Задірака, О.С. Олексюк. – К.: Вища шк., 2000. – 460 с.

Література знаходиться на кафедрі та у студентів у електронному вигляді. Викладач проводить індивідуальне консультування студентів у визначених розкладом часі та аудиторії.

VI. Мова

Дисципліна викладається українською мовою.

VII. Характеристика індивідуальних завдань

Студентам пропонується виконати і захистити індивідуальні семестрові завдання у формі контрольних індивідуальних завдань, що супроводжують підготовку до виконання лабораторних робіт формуючи певні навички та вміння, відповідно до ОПП. Основними цілями індивідуальних семестрових завдань є: засвоєння студентами знань з основних тем дисципліни та їх закріплення; формування у студентів навичок і вмінь з виконання обрахунків у межах основних тем, та виконання процедур та алгоритмів кодоперетворення (шифрування та дешифрування) даних основними типами криптошифрів та цифрового підпису; формування у студентів навичок і вмінь з розробки алгоритмів, написання та налаштування кодів програм у межах основних тем з шифрування та дешифрування даних основними типами криптошифрів, цифрового підпису документа та верифікації ЕЦП.

Індивідуальні семестрові завдання пропонують студентові виконати процедури шифрування та дешифрування висхідних даних криптошифрами, що він вивчає в дисципліні, а також теоретичну їх оцінку; розробити алгоритми, написати та налаштувати коди програм у межах основних тем. Перелік тих шифрів має бути вказаний викладачем в завданні.

Приблизна тематика індивідуальних семестрових завдань:

- Шифр Цезаря. Шифр Тритеміуса. Шифр Гамірування.
- Шифр Віжинера.
- Шифр зі штучним алфавітом.
- Шифр DES. Шифр 2DES. Шифр 3DES.
- Шифр ГОСТ 28147-89.
- Алгоритми Blowfish, Twofish.
- Шифр AES.
- Hash-сума. MD5.
- Арифметична система GF(p). Скінчені поля Галуа.
- Криптосистема Diffie - Hellman.
- Криптосистема RSA.
- Криптосистема El Gamal.

- Система ЕЦП Hash-RSA, DSS (DSA).
- Система ЕЦП на еліптичних кривих.
- Протоколи аутентифікації PAP, CHAP та інші.
- Протокол аутентифікації Kerberos.
- Протокол аутентифікації TACACS.
- Протокол аутентифікації RADIUS.
- Інфраструктура сертифікатів відкритих ключів X.509.

VIII. Методика оцінювання

Оцінювання знань та вмінь студента виконується за наступною методикою:

1. Враховується окремо кількість занять, які відвідав студент окремо за видами – лекція, лабораторний комп'ютерний практикум, МКР.
2. Призначається максимальна кількість балів за одне повністю виконане заняття: лекція – 4 бал, лабораторний комп'ютерний практикум – 6 балів (3 бали за виконання лаб. практ. + 3 бали за підготовку інд. завд. до лаб. практ.), 10 балів за МКР.
3. Обраховується вся сума набраних балів за дійсно виконані завдання з урахуванням їх якості

$$N = L1*B1 + L2*B2 + L3*B3 - S,$$

де Li - кількість занять, які відвідав студент, i = 1 – лекція, i = 2 – лабораторний комп'ютерний практикум, i = 3 – МКР; Bi – кількість балів за одне повністю виконане заняття, S - штрафні бали за недовиконання завдань. Максимальна сума складає 100 балів.

4. Обраховується відсоток виконання навчальної програми за формулою:

Оцінка **O = (N / 100)*100%.**

Нижче наведені приклади розрахунку оцінки студента на заліку за умов повного виконання програми навчання, та неповного виконання (менша кількість відпрацьованих занять, без штрафних балів).

Повний розрахунок оцінки студента на заліку при умові, що він відвідав усі заплановані розкладом заняття та виконав усі завдання з дисципліни

		Li				**Bi**	**Si**		
№	Вид	Кількість	Лаб.пркт.	Практ.	Інд.завд.	балів за	Штрафні бали	Сума	
	занять	занять	балів	балів	балів	1 зан		за вид	
1	лекція	9				4	-1	36	
2	лаб. практ.	9	3		3	6	-1…-2	54	
4	МКР	1				10	-1…-5	10	
								Оцінка **O**	
					N =	Всього:	100	дорівнює	100%

Перевірний варіант: Студент відвідав меншу кількість занять

Приклад припустимої межі для заліку

№	Вид занять	Кількість занять	Лаб.пркт. занять	Практ. занять	Інд.завд. занять	балів за 1 зан	Штрафні бали	Сума за вид	
1	лекція	5				4	-1	20	
2	лаб. практ.	5	3		3	6	-1…-2	30	
3	МКР	1				10	-1…-5	10	
								Оцінка **О**	
					N =	Всього:	60	дорівнює	60%

IX. Організація

У випадках, де наявність вибіркових кредитних модулів програми підготовки може залежати від мінімальної кількості студентів.