ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету IT
_____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«31» 08 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія криптосистем та управління криптографічними ключами

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека та захист інформації
Рівень вищої освіти	Другий магістерський
Освітньо-професійна програма	Кібербезпека та захист інформації
Обсяг дисципліни	5 кредитів ЄКТС
Шифр дисципліни	ОПП.04
Мова навчання	Українська
Статус дисципліни	Обов'язкова, дисципліна професійної підготовки
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Очна (денна)	1	2	5	150	54	18	36			96				+

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації»

Робоча програма складена _____ д-р. техн. наук, проф. Михайло КАСЯНЧУК
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 31.08.2023 № 1 Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2023

ТЕОРІЯ КРИПТОСИСТЕМ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ

Тип дисципліни	Обов'язкова
Освітній рівень	Другий (магістерський)
Мова викладання	Українська
Семестр	Другий
Кількість встановлених кредитів ЄКТС	5
Форми навчання, для яких викладається дисципліна	Денна

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати*, *інтегрувати*, *розробляти* та *удосконалювати* сучасні інформаційні технології для провадження інноваційної діяльності в сфері інформаційної безпеки та/або кібербезпеки, криптографічного захисту інформації у кіберпросторі; *досліджувати* та *розробляти* засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури; *досліджувати*, *розробляти*, *впроваджувати* та *використовувати* методи та засоби криптографічного захисту інформації бізнес/операційних процесів, а також *аналізувати* і *надавати* оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури; *обирати*, *аналізувати* і *розробляти* придатні типові аналітичні, розрахункові та експериментальні методи криптографічного захисту інформації.

Зміст навчальної дисципліни. Підходи до реалізації сучасних криптографічних систем та протоколів. Квантова криптографія. Проєктування криптосистем RSA та Ель-Гамаля на основі векторномодульного-методу модулярного множення та експоненціювання. Теоретичні основи системи залишкових класів. Методи проєктування криптосистем на основі залишкових класів. Застосування методів криптоаналізу. Управління ключами. Інфраструктура відкритих ключів. Створення центру сертифікації ключів.

Пререквізити – вихідна

Кореквізити – професійна практика

Запланована навчальна діяльність: лекції – 18 год., лабораторні заняття – 36 год., самостійна робота – 96 год.; разом – 150 год.

Методи навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Форми оцінювання результатів навчання: захист лабораторних робіт, контрольна робота, підсумковий контрольний захід.

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». Тернопіль. 2020. 380 с.
2. Досконала форма системи залишкових класів: методи проєктування та застосування: монографія/ М. М. Касянчук. Тернопіль: ТНЕУ, 2019. 223 с.
3. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
5. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua
6. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php

Викладач: д.т.н., професор Касянчук М.М.

ВСТУП

Дисципліна «Теорія криптосистем та управління криптографічними ключами» - складова професійної підготовки магістрів зі спеціальності «Кібербезпека та захист інформації».

Метою викладання навчальної дисципліни є формування у майбутніх спеціалістів умінь та компетенцій для розробки і супроводу методів та засобів криптографічного захисту інформації; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань впровадження методів за засобів криптографічного захисту на об'єктах інформаційної діяльності.

Предметом дисципліни є технології, методи та засоби інформаційної безпеки та/або кібербезпеки, криптографічне програмне та програмно-апаратне забезпечення (засоби) кіберзахисту.

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до освітньо-професійної програми підготовки магістрів зі спеціальності «Кібербезпека та захист інформації»:

компетентності:

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

результати навчання:

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проєкти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати, інтегрувати, розробляти* та *удосконалювати* сучасні інформаційні технології для провадження інноваційної діяльності в сфері інформаційної безпеки та/або кібербезпеки, криптографічного захисту інформації у кіберпросторі; *досліджувати* та *розробляти* засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури; *досліджувати, розробляти, впроваджувати* та *використовувати* методи та засоби криптографічного захисту інформації бізнес/операційних процесів, а також *аналізувати* і *надавати* оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури; *обирати, аналізувати* і *розробляти* придатні типові аналітичні, розрахункові та експериментальні методи криптографічного захисту інформації.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	**Кількість годин відведених на:**		
	лекції	**лабораторні роботи**	**самостійну роботу**
Тема 1. Теорія криптографічних систем	8	24	56
Тема 2. Управління криптографічними ключами	6	12	40
Разом:	**18**	**36**	**96**

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотація	Години
	Тема 1. Теорія криптографічних систем	
1	**Підходи до реалізації сучасних криптографічних систем та протоколів** 1. Проєктування криптосистем за принципом Керкгоффса. 2. Розробка та моделювання сучасних криптографічних протоколів. 3. Підхід до формування протоколів цифрового підпису різного призначення (сліпий підпис, колективний підпис тощо). 4. Аналіз алгоритмів заперечного шифрування та їх модифікація. Літ.: [1] с. 17-26; [3] с. 280-292; [4] с. 33-39, 43-45; [5] с. 56-75; [18]; [19]; [20]; [25]	2
2	**Квантова криптографія** 1. Дослідження переваг використання квантової криптографії. 2. Розробка паралельних моделей протоколів квантової криптографії під технологію GPGPU. 3. Порівняльний аналіз протоколів квантового розподілення ключів. 4. Моделювання протоколів квантової криптографії на платформі CUDA. Літ.: [4] с. 45-53; [10] с. 9-88; [11]	2
3	**Проєктування криптосистем RSA та Ель-Гамаля на основі векторномодульного-методу модулярного множення та експоненціювання** 1. Теоретичні основи векторно-модульного-методу модулярного множення та експоненціювання. 2. Проєктування криптосистеми RSA на основі векторно-модульного-методу модулярного множення та експоненціювання. 3. Проєктування криптосистеми Ель-Гамаля на основі векторно-модульногометоду модулярного множення та експоненціювання Літ.: [8] с. 92-130; [9] с. 33-51; [21]; [22]; [23]; [24]	2
4	**Теоретичні основи системи залишкових класів** 1. Теоретичні основи системи залишкових класів 2. Методи відновлення десяткового числа за його залишками. Китайська теорема про остачі. 3. Методи проєктування досконалої та модифікованої досконалої форм системи залишкових класів. Літ.: [2] с. 55-80; [9] с. 51-73; [21]; [22]; [23]; [24]	2
5	**Методи проєктування криптосистем на основі залишкових класів** 1. Методи проєктування симетричних криптосистем на основі залишкових класів. 2. Методи проєктування асиметричних криптосистем на основі залишкових класів 3. Використання модифікованої досконалої форми системи залишкових класів для проєктування криптосистем. Літ.: [9] с. 51-73; [12]; [13]; [21]; [22]; [23]; [24]	2
6	**Застосування методів криптоаналізу** 1. Класифікація криптоаналітичних атак. 2. Клептографічні атаки на криптосистеми та захист від них. 3. Нові технології у криптоаналізі (нейронні мережі, генетичні алгоритми, квантові комп'ютери). Літ.: [2] с. 220-247; [3] с. 36-42, 127-131, 216-228, 370-383, 418-430; [4] с.	2

	39-43; [5] с. 6-56; [14]	
Тема 2. Управління криптографічними ключами		
7	**Управління ключами** 1. Аналіз цілей управління ключами. 2. Особливості політики безпеки управління ключами (термін дії ключів, життєвий цикл ключів, послуги, що надаються довіреною третьою стороною). 3. Процеси впровадження систем умовного депонування ключів підприємства для підтримки шифрування даних у стані спокою [6] с. 315-371; [7] с. 420-453, 481-530; [15]	2
8	**Інфраструктура відкритих ключів** 1. Проєктування, впровадження та супровід захищених систем доменних імен DNS. 2. Проєктування, впровадження та супровід систем захищеної електронної пошти PGP. 3. Проєктування, впровадження та супровід систем захищених електронних транзакцій SET. 4. Інфраструктура відкритих ключів Oauth, OpenID, SAML, SPML. Літ.: [7] с. 297-387; [16]; [17]; [26]	2
9	**Створення центру сертифікації ключів (ЦСК)** 1. Категоріювання та обстеження ЦСК. Підготовка організаційно-розпорядчої документації. 2. Проєктування, створення та впровадження ЦСК. Структура та склад центру. 3. Особливості проектування ЦСК на базі криптомодулів. 4. Розробка програми та супровід внутрішніх випробувань. Дослідна експлуатація. 5. Планування навчання обслуговуючого персоналу. 6. Експертизи та акредитація ЦСК. Літ.: [7] с. 387-420, 453-481	2
	Разом за семестр:	**18**

Зміст лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
1	Проєктування криптосистем сучасними програмними та апаратними засобами Літ.: [2] с. 155-191	4
2	Проєктування криптосистем на основі електронного цифрового підпису Літ.: [2] с. 272-284, 308-325	4
3	Проєктування криптосистем для аутентифікації повідомлень Літ.: [2] с. 284-308	4
4	Проєктування та модифікація криптосистем на основі заперечуваного шифрування Літ.: [4] с. 43-45	4
5	Проєктування криптосистем на основі векторно-модульного методу модулярного множення та експоненціювання Літ.: [8] с. 92-130	4
6	Проєктування криптосистем на основі системи залишкових класів Літ.: [9] с. 51-73	4
7	Аналіз стійкості криптосистем за допомогою нейронних мереж Літ.: [5] с. 50-51	4
8	Аналіз стійкості криптосистем за допомогою генетичних алгоритмів Літ.: [5] с. 51-53	4
9	Підсумкове заняття. Контрольна робота	4
	Разом за семестр:	**36**

Зміст самостійної (у т.ч. індивідуальної) роботи

Об’єм самостійної роботи з дисципліни становить 96 годин. Він включає опрацювання лекційного матеріалу та літературних джерел, підготовку до тестування, підготовку до виконання та захисту лабораторних робіт. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

№ тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1.	5
2	Підготовка до виконання лабораторної роботи №1	5
3	Опрацювання теоретичного матеріалу лекції №2.	5
4	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	6
5	Опрацювання теоретичного матеріалу лекції №3.	5
6	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	6
7	Опрацювання теоретичного матеріалу лекції №4.	5
8	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	6
9	Опрацювання теоретичного матеріалу лекції №5.	5
10	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	6
11	Опрацювання теоретичного матеріалу лекції №6.	5
12	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	6
13	Опрацювання теоретичного матеріалу лекції №7.	5
14	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	6
15	Опрацювання теоретичного матеріалу лекції №8.	5
16	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	6
17	Опрацювання теоретичного матеріалу лекції №9.	5
18	Підготовка до захисту лабораторної роботи №8. Підготовка до контрольної роботи за пройденим матеріалом.	4
	Разом за семестр:	96

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції пояснювально-ілюстративними та проблемними методами з супроводом презентаційних матеріалів, лабораторні роботи проводяться з використанням практичних, продуктивних, проблемних та контекстних методів, методами моделювання та з застосуванням сучасних інформаційно-комп'ютерних технологій і мають за мету набуття студентами практичних навичок розробки, впровадження і супроводу методів та засобів криптографічного захисту інформації.

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: обговорення проблемних питань під час лекцій, прилюдні захисти лабораторних робіт з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни; обмежений час на виконання лабораторних робіт і контрольних завдань, чітко визначені і надані в силабусі терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ.

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- захист лабораторних робіт;
- контрольна робота.

Семестровий контроль проводиться у формі іспиту. При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контрольного заходу.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1-2	1-2	1-2
Ваговий коефіцієнт	0,3	0,3	0,4

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторну роботу, складається з таких елементів: знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторну роботу викладач оголошує одразу після захисту звіту і проставляє в електронний журнал дисципліни.

Оцінювання контрольних робіт. Контрольна робота складається з двох теоретичних питань. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичні питання.

Оцінку «добре» отримує студент, який дав правильну відповідь на теоретичні питання, але у відповіді присутні дві-три несуттєві помилки.

Оцінку «задовільно» отримує студент, який дав часткову відповідь на теоретичні питання.

Оцінку «незадовільно» отримує студент, який не дав відповіді на теоретичні питання.

Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення контрольного заходу.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з теоретичного питання і задачі. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

Засвоєння студентом матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального

	матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка «задовільно».

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**	
A	4,75–5,00	5	***Відмінно*** – глибоке і повне опанування навчального

			матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4	***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4	***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3	***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3	***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2	***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Основні визначення криптографічних послуг безпеки.
2. Математичні методи сучасної інформаційної безпеки.
3. Принцип Керкгоффса.
4. Види криптографічних протоколів.
5. Властивості, що визначають безпеку криптографічних протоколів.
6. Аналіз і моделювання криптографічних протоколів.
7. Центр сертифікації ключів.
8. Кореневий центр сертифікації.
9. Кроссертифікація.
10. Сертифікат X.509 v3.
11. Список відкликаних сертифікатів. Причини відкликання сертифікату.
12. Протокол OCSP (Online Certificate Status Protocol).
13. Криптоаналітичні атаки та класи стійкості шифрів.
14. Атаки на схеми шифрування.
15. Атака вичерпного пошуку та словникова атака.
16. Атака на основі застосування таблиць передобчислень.
17. Атака розширення довжини на конструкцію Меркля-Дамгарда.
18. Атака «зустріч посередині» на шифр з відкритим ключем.
19. Застосування слабкого протоколу управління ключами.
20. Ідеальний шифр, принципи проєктування та властивості.
21. Безумовно стійкі та практично (обчислювально) стійкі шифри.
22. Метод грубої сили.
23. Парадокс днів народження.
24. Диференційний аналіз.
25. Лінійний аналіз.
26. Метод відпалу.
27. Методи визначення простоти чисел.
28. Методи факторизації великих чисел.
29. Методи цілочислового логарифмування.
30. Алгорим Полларда.
31. Алгоритм Ленстра.
32. Алгоритм факторизації на основі рішення нерівності.
33. Алгоритм дискретного логарифмування.
34. Алгоритм решета числового поля.
35. Криптоаналіз систем на еліптичних кривих.
36. Програмні шифратори, переваги та недоліки.
37. Апаратні шифратори, структура та проблеми застосування.
38. Шифратори для захисту мереж.
39. Криптографічні модулі, їх застосування в задачах криптографічної безпеки.
40. Особливості застосування шифраторів та криптомодулів на об’єктах критичної інфраструктури.
41. Встановлення захищеного каналу. Встановлення доступу до інформації.
42. Сегментування віртуальних машин.
43. Аутентифікація даних і електронний цифровий підпис.
44. Інтелектуальні засоби для криптоаналізу шифрів.
45. Апаратний криптографічний захист. Криптосистема на основі IP-шифраторів.
46. Апаратний криптографічний захист. Криптосистема на основі криптомодулів.
47. Теоретичні основи векторно-модульного-методу модулярного множення та експоненціювання.

48. Проєктування криптосистеми RSA на основі векторно-модульного-методу медулярного множення та експоненціювання.
49. Проєктування криптосистеми Ель-Гамаля на основі векторно-модульного-методу модулярного множення та експоненціювання.
50. Теоретичні основи системи залишкових класів.
51. Методи відновлення десяткового числа за його залишками. Китайська теорема про остачі.
52. Методи проєктування досконалої та модифікованої досконалої форм системи залишкових класів.
53. Методи проєктування симетричних криптосистем на основі залишкових класів.
54. Методи проєктування асиметричних криптосистем на основі залишкових класів.
55. Використання модифікованої досконалої форми системи залишкових класів для проєктування криптосистем.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Технології захисту інформації/ Ю. А. Тарнавський. Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с.
2. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші ; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
3. Прикладна криптологія: системи шифрування: підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. К.: ДУТ, 2014. 448 с.
4. Звіт про науково-дослідну роботу дослідження і розробка криптографічних та технічних методів захисту інформації/ Л.М. Карпуков, С.І. Лізунов, В.О. Воскобойник та інші. Запорізький національний технічний університет, 2018. 91 с.
5. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
6. Технології захисту інформації : навчальний посібник/ С. Е. Остапов, С. П. Євсеєв, О. Г. Король. Х. : Вид. ХНЕУ, 2013. 476 с.
7. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика/ Ю.І. Горбенко, І.Д. Горбенко. К.: ДУТ, 2010. 580 с.
8. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». Тернопіль. 2020. 380 с.
9. Досконала форма системи залишкових класів: методи проєктування та застосування: монографія/ М. М. Касянчук. Тернопіль: ТНЕУ, 2019. 223 с.
10. Квантова інформатика та квантові обчислення/ С.Е.Остапов. Ю.Г. Добровольський. Чернівці: ЧНУ, 2021. 99 с.

Додаткова

11. Modern developed of post-quantum safety of state-owned electronic information resources/ A. Korchenko, Ye. Ivanchenko, N. Koshkina, O. Kuznetsov, O. Kachko, O. Potiy, V. Onoprienko, V. Bobukh// Ukrainian Scientific Journal of Information Security, 2021, vol. 26, issue 1. pp. 27-52.
12. Асиметричні алгоритми шифрування у системі залишкових класів/ Я.М. Николайчук, І.З. Якименко, Н.Я. Возна, М.М. Касянчук // Кібернетика і системний аналіз, №4, Т.58. 2022. С. 129-138.
13. Symmetric Cryptoalgorithms in the Residue Number System/ Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko// Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.
14. Preventing fault attacks using fault randomisation with a case study on AES/ Shamit Ghosh; Dhiman Saha; Abhrajit Sengupta; Dipanwita Roy Chowdhury. International Journal of Applied Cryptography, 2017, Vol.3, No.3. PP.225-235. DOI: 10.1504/IJACT.2017.086231
15. Методи, методика та результати порівняльного аналізу електронних підписів згідно з ДСТУ ISO/IEC 14888-3:2014/ І. Д. Горбенко, М. В. Єсіна// Вісн. Нац. ун-ту "Львів. політехніка". 2016. № 852. С. 9-22.
16. Використання технології DNSSEC для захисту доменних імен в українському сегменті мережі Інтернет/ В.Зубок// Information Technology and Security. July-December 2017. Vol. 5. Iss. 2 (9). С. 43-50.

17. A privacy-enhanced access log management mechanism in SSO systems from nominative signatures/ Sanami Nakagawa; Takashi Nishide; Eiji Okamoto; Keita Emura; Goichiro Hanaoka; Yusuke Sakai; Akihisa Kodate. – International Journal of Applied Cryptography, 2017, Vol.3, No.4. PP. 394 406. DOI: 10.1504/IJACT.2017.089373
18. Sponge-based CCA2 secure asymmetric encryption for arbitrary length message (extended version)/ Tarun Kumar Bansal; Donghoon Chang; Somitra Kumar Sanadhya. - International Journal of Applied Cryptography, 2017, Vol.3, No.3. PP. 262-287. DOI: 10.1504/IJACT.2017.086222
19. Cryptology and information security - past, present, and future role in society/ S. Bhattacharya. International Journal on Cryptography and Information Security (IJCIS). Vol. 9, No.1/2, 2019. P. 13-36.
20. Cryptology and communication security [Електронний ресурс]/ Shri Kant. Defense Science Journal. Vol. 62. №1. Режим доступу: https://core.ac.uk/reader/333719963
21. Модифікований метод шифрування Рабіна з використанням різних форм системи залишкових класів/ М.М. Касянчук, І.З. Якименко, Л.О. Дубчак, Н.А. Рендзеняк, Н.М. Мандебура. Вісник Хмельницького національного університету. Технічні науки №1, 2017. С. 127-131.
22. Вибір параметрів еліптичних кривих у задачах шифрування інформаційних потоків/ І.З. Якименко, Л.М. Тимошенко, М.М. Касянчук. Сучасна спеціальна техніка, №2, 2018. С. 63-71.
23. Методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах/ М. М. Касянчук, М. П. Карпінський, С. В. Казмірчук. Захист інформації, №2, т.21, 2019. С. 65-73
24. Розробка трьохмодульної криптосистеми Рабіна на основі операції додавання/ М.М. Касянчук, О.Я. Лотоцький, С.В. Яцків, С.В. Івасьєв, Л.М. Тимошенко. Informatics & Mathematical Methods in Simulation, №11, 2021. С. 47-57.
25. Симетрична система з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування/ В.М. Джулій, І.В. Муляр, В.С. Орленко, В.Ю. Тітова, В.А. Анікін// Вісник Хмельницького національного університету. Технічні науки. 2020. № 6. С. 33-39.
26. Altice Labs Whitepaper. Identity and Access Management. [Електронний ресурс]. Режим доступу: https://www.openlabs.com.br/content/WP-Information-Access-Control-Models.pdf

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/
2. Електронна бібліотека університету. URL: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php