ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
Тетяна ГОВОРУЩЕНКО
«31» 08 2024 р.

СИЛАБУС

Навчальна дисципліна: "*Теорія криптосистем та управління криптографічними ключами*"

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: другий (магістерський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Касянчук Михайло Миколайович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/sklad-kafedry/
E-mail викладача(ів)	kasjanchukmm@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=7850
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us05web.zoom.us/j/7943096545 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр II (зимово-весняний)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
ОД	1	2	5	150	54	18	36	-	-	96	-	-	-	+

Анотація дисципліни

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека та захист інформації». При викладанні дисципліни використовуються наступні форми (методи) навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Пререквізити – вихідна

Кореквізити – професійна практика.

Мета і завдання дисципліни

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.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна роботи		
			Зміст	Год.	Література
1	**Тема 1. Теорія криптографічних систем** Підходи до реалізації сучасних криптографічних систем та протоколів	**ЛР1.** Проєктування криптосистем сучасними програмними та апаратними засобами	Опрацювання теоретичного матеріалу лекції №1.	5	[1] с. 17-26 [3] с. 280-292 [4] с. 33-39, 43-45 [5] с. 56-75 [18] [19] [20] [25]
2	-	**ЛР1.** Підгрупа 2	Підготовка до виконання лабораторної роботи №1	5	[2] с. 155-191
3	**Тема 1. Теорія криптографічних систем** Квантова криптографія	**ЛР2.** Проєктування криптосистем на основі електронного цифрового підпису	Опрацювання теоретичного матеріалу лекції №2.	5	[4] с. 45-53 [10] с. 9-88 [11]
4	-	**ЛР2.** Підгрупа 2	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	6	[2] с. 155-191, 272-284, 308-325
5	**Тема 1. Теорія криптографічних систем** Проєктування криптосистем RSA та Ель-Гамаля на основі векторномодульного-методу модулярного множення та експоненціювання	**ЛР3.** Проєктування криптосистем для аутентифікації повідомлень	Опрацювання теоретичного матеріалу лекції №3.	5	[8] с. 92-130 [9] с. 33-51 [21] [22] [23] [24]
6	-	**ЛР3.** Підгрупа 2	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	6	[2] с. 272-325
7	**Тема 1. Теорія криптографічних систем** Теоретичні основи системи залишкових класів	**ЛР4.** Проєктування та модифікація криптосистем на основі заперечуваного шифрування	Опрацювання теоретичного матеріалу лекції №4.	5	[2] с. 55-80 [9] с. 51-73 [21] [22] [23] [24]
8	-	**ЛР4.** Підгрупа 2	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	6	[2] с. 284-308 [4] с. 43-45

9	**Тема 1. Теорія криптографічних систем** Методи проєктування криптосистем на основі залишкових класів	**ЛР5.** Проєктування криптосистем на основі векторно-модульного методу модулярного множення та експоненціювання	Опрацювання теоретичного матеріалу лекції №5.	5	[9] с. 51-73 [12] [13] [21] [22] [23] [24]
10	-	**ЛР5.** Підгрупа 2	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	6	[4] с. 43-45 [8] с. 92-130
11	**Тема 1. Теорія криптографічних систем** Застосування методів криптоаналізу	**ЛР6.** Проєктування криптосистем на основі системи залишкових класів	Опрацювання теоретичного матеріалу лекції №6.	5	[2] с. 220-247 [3] с. 36-42, 127-131, 216-228, 370-383, 418-430 [4] с. 39-43 [5] с. 6-56 [14]
12	-	**ЛР6.** Підгрупа 2	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	6	[8] с. 92-130 [9] с. 51-73
13	**Тема 2. Управління криптографічними ключами** Управління ключами	**ЛР7.** Аналіз стійкості криптосистем за допомогою нейронних мереж	Опрацювання теоретичного матеріалу лекції №7.	5	[6] с. 315-371 [7] с. 420-453, 481-530 [15]
14	-	**ЛР7.** Підгрупа 2	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	6	[5] с. 50-51 [9] с. 51-73
15	**Тема 2. Управління криптографічними ключами** Інфраструктура відкритих ключів	**ЛР8.** Аналіз стійкості криптосистем за допомогою генетичних алгоритмів	Опрацювання теоретичного матеріалу лекції №8.	5	[7] с. 297-387 [16] [17] [26]
16	-	**ЛР8.** Підгрупа 2	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	6	[5] с. 50-53
17	**Тема 2. Управління криптографічними ключами** Створення центру сертифікації ключів (ЦСК)	-	Опрацювання теоретичного матеріалу лекції №9.	5	[7] с. 387-420, 453-481

18	-	Підсумкове заняття **Контрольна робота**	Підготовка до захисту лабораторної роботи №8. Підготовка до контрольної роботи за пройденим матеріалом.	4	[5] с. 51-53

*** лекції проводяться по 2 години раз на два тижні;**
**** лабораторні проводяться по 4 години раз в два тижні.**

ПОЛІТИКА ДИСЦИПЛІНИ

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і лабораторні заняття згідно з розкладом, не запізнюватися на заняття, вчасно виконувати та здавати лабораторні роботи. Термін виконання лабораторної роботи вважається своєчасним, якщо студент здав/захистив її на поточному або наступному за ним занятті. За несвоєчасний захист лабораторної роботи з набраної студентом суми балів вираховується один бал. Пропущене з поважної причини лабораторне заняття студент повинен відпрацювати у встановлений викладачем термін.

Виконуючи усі навчальні завдання з дисципліни, студент має дотримуватися політики доброчесності. У разі наявності плагіату він отримує незадовільну оцінку і має виконати завдання за новою темою.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок визнання та перезарахування результатів навчання здобувачів вищої освіти у ХНУ.

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 теоретичного питання та задачі. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичне питання та правильно вирішив задачу, з обґрунтуванням вибору методів для його розв'язування.

Оцінку «добре» отримує студент, який дав правильну відповідь на теоретичне питання та правильно вирішив задачу, але у відповіді присутні дві-три несуттєві помилки, або є вагання з обґрунтуванням вибору методів вирішення.

Оцінку «задовільно» отримує студент, який дав часткову відповідь на теоретичне питання та допустив суттєві помилки при вирішення задачі.

Оцінку «незадовільно» отримує студент, який не зміг обрати правильні методи для вирішення задачі або не дав відповіді на теоретичне 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. Класифікація малоресурсних криптографічних систем. Види шифрів.
14. Криптоакселератори шифрування.
15. Криптоаналітичні атаки та класи стійкості шифрів.
16. Атаки на схеми шифрування.
17. Атака вичерпного пошуку та словникова атака.
18. Атака на основі застосування таблиць передобчислень.
19. Атака розширення довжини на конструкцію Меркля-Дамгарда.
20. Атака «зустріч посередині» на шифр з відкритим ключем.
21. Застосування слабкого протоколу управління ключами.
22. Ідеальний шифр, принципи побудови та властивості.
23. Безумовно стійкі та практично (обчислювально) стійкі шифри.
24. Метод грубої сили.
25. Парадокс днів народження.
26. Диференційний аналіз.
27. Лінійний аналіз.
28. Метод відпалу.
29. Методи визначення простоти чисел.
30. Методи факторизації великих чисел.
31. Методи цілочислового логарифмування.
32. Алгорим Полларда.
33. Алгоритм Ленстра.
34. Алгоритм факторизації на основі рішення нерівності.
35. Алгоритм дискретного логарифмування.
36. Алгоритм решета числового поля.
37. Криптоаналіз систем на еліптичних кривих.
38. Програмні шифратори, переваги та недоліки.
39. Апаратні шифратори, структура та проблеми застосування.
40. Шифратори для захисту мереж.
41. Криптографічні модулі, їх застосування в задачах криптографічної безпеки.
42. Особливості застосування шифраторів та криптомодулів на об’єктах критичної інфраструктури.
43. Встановлення захищеного каналу. Встановлення доступу до інформації.
44. Сегментування віртуальних машин.
45. Методика шифрування. Гомоморфне шифрування.
46. Технологія Blockchain. Принципи технології довіри. Структура блоку. Заголовок блоку. Блок генезису. Алгоритми доказу виконаної роботи.
47. Аутентифікація даних і електронний цифровий підпис.
48. Інтелектуальні засоби для криптоаналізу шифрів.
49. Апаратний криптографічний захист. Криптосистема на основі IP-шифраторів.

50. Апаратний криптографічний захист. Криптосистема на основі криптомодулів.
51. Теоретичні основи векторно-модульного-методу модулярного множення та експоненціювання.
52. Побудова криптосистеми RSA на основі векторно-модульного-методу модулярного множення та експоненціювання.
53. Побудова криптосистеми Ель-Гамаля на основі векторно-модульного-методу модулярного множення та експоненціювання.
54. Теоретичні основи системи залишкових класів.
55. Методи відновлення десяткового числа за його залишками. Китайська теорема про остачі.
56. Методи побудови досконалої та модифікованої досконалої форм системи залишкових класів.
57. Методи побудови симетричних криптосистем на основі залишкових класів.
58. Методи побудови асиметричних криптосистем на основі залишкових класів.
59. Використання модифікованої досконалої форми системи залишкових класів для побудови 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. Тітова В.Ю. Проектування складових архітектури комп'ютерів мовою VHDL: Навч. посібник для ВНЗ. Хмельницький: ФОП А.С. Гонта, 2018. 264 с.
5. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
6. 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.
7. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика/ Ю.І. Горбенко, І.Д. Горбенко. К.: ДУТ, 2010. – 580 с.
8. Методи побудови та дослідження властивостей малоресурсних блокових шифрів та їх компонентів/ М.Ю. Родінко. Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття ступеня доктора філософії за спеціальністю 122. Комп'ютерні науки. Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України, Харків, 2020. 201 с.
9. Power and Energy issues on lightweight cryptography/ Antonio J. Acosta, Erica Tena-Sánchez, Carlos J. Jiménez, José M. Mora. - Instituto de Microelectrónica de Sevilla, Universidad de Sevilla/CSIC, Spain. September 2017. Journal of Low Power Electronics 13(3):326-337 DOI:10.1166/jolpe.2017.1490
10. 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
11. Хмарні технології. Навчальний посібник/ О.В. Зінченко, С.М. Іщеряков, С.В. Прокопов, С.О. Сєрих, В.В. Василенко. К: ФОП Гуляєва В.М., 2020. 74 с.
12. Анна Ільєнко. Сучасні методи гомоморфного шифрування інформаційних ресурсів. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (30), 2015 р. с. 52-57.
13. 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.
14. Теоретичні аспекти сучасних систем документообігу та документообміну на приватних підприємствах [Електронний ресурс]. Режим доступу: http://www.dut.edu.ua/uploads/p_421_86928920.pdf
15. 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.
16. 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
17. Attribute-based fully homomorphic encryption with a bounded number of inputs/ Michael Clear; Ciarán Mc Goldrick. International Journal of Applied Cryptography, 2017, Vol.3, No.4. pp.363-376. DOI: 10.1504/IJACT.2017.089356
18. Efficient coding for secure computing with additively-homomorphic encrypted data/ Thijs Veugen. - International Journal of Applied Cryptography, 2020, Vol.4, No.1. pp.1-15. DOI: 10.1504/IJACT.2020.107160
19. A new public remote integrity checking scheme with user and data privacy/ Yiteng Feng; Guomin Yang; Joseph K. Liu. International Journal of Applied Cryptography, 2017, Vol.3, No.3. pp.196- 209. DOI: 10.1504/IJACT.2017.086232
20. 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
21. A new authenticated encryption technique for handling long ciphertexts in memory constrained devices/ Megha Agrawal; Donghoon Chang; Somitra Kumar Sanadhya. International Journal of Applied Cryptography, 2017, Vol.3, No.3. pp. 236-261. DOI: 10.1504/IJACT.2017.086223
22. 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
23. CCA-secure revocable identity-based encryption schemes with decryption key exposure resistance/ Yuu Ishida; Junji Shikata; Yohei Watanabe. International Journal of Applied Cryptography, 2017, Vol.3, No.3. pp. 288-311. DOI: 10.1504/IJACT.2017.086229
24. 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.
25. Досконала форма системи залишкових класів: методи побудови та застосування: монографія/ М. М. Касянчук. Тернопіль: ТНЕУ, 2019. 223 с.
26. 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.
27. 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.

Додаткова

28. A Review of RSA Cryptosystems and Cryptographic Protocols/ P. O. Asagba, E. Nwachukwu// West African Journal of Industrial & Academic Research. Vol.10 No.1. 2014. p. 3-16.
29. Hybrid cryptographic technique using rsa algorithm and scheduling concepts/ M. Shankar, P. Akshaya// International Journal of Network Security & Its Applications (IJNSA)/ Vol.6, No.6. 2014. p. 39-48
30. Sequence Alignment with Dynamic Divisor Generation for Keystroke Dynamics Based User Authentication/ Jiacang Ho, Dae-Ki Kang// Hindawi Publishing Corporation, Journal of Sensors. 2015. p. 1-14.
31. Elliptic Curve Cryptology [Електронний ресурс]/ F. Rocco. Union College. Schenectady, NY, 2017.
32. 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.
33. 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.

34. 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.
35. 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
36. 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.
37. 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.

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
3.