



КІБЕРБЕЗПЕКА ФІНАНСОВИХ СИСТЕМ

Викладач: д.ф.-м.н., Козін Ігор Вікторович

Кафедра: економічної кібернетики, V корпус, ауд. 113

E-mail: odvisua@gmail.com

Телефон: (061) 228-76-41 (кафедра)

Інші засоби зв'язку: Moodle (форум курсу, приватні повідомлення)

Освітні програми		Економічна кібернетика					
Рівень вищої освіти		Бакалаврський					
Статус дисципліни		Вибіркова					
Кредити ECTS	3	Рік набру	2023	Рік навчання -3	Сем естр - 6	Тижні	14
Кількість годин	90	Кількість змістових модулів¹		4	Лекційні заняття – 14 Лабораторні заняття - 14 Самостійна робота – 52		
Вид контролю	Залік						
Посилання на курс в Moodle			https://moodle.znu.edu.ua/course/view.php?id=3029				
Консультації:			2 год. на тиждень, за розкладом (особисто); за домовленістю (особисто чи дистанційно)				

ОПИС КУРСУ

Метою викладання навчальної дисципліни «Кібербезпека фінансових систем» є формування базових знань з основ криптографічного захисту інформації, знайомство з сучасними алгоритмами шифрування інформації, теорією цифрового підпису, уміння будувати захищені інформаційні системи для обробки економічної інформації.

Об'єктом вивчення дисципліни є інформаційні системи, бази даних, інші сховища інформації, системи передачі інформації.

Предметом курсу є основні теоретичні результати і методи сучасної криптографії, їх застосування до побудови захищених інформаційних систем, та захисту інформації, що передається по каналах зв'язку.

Основними **завданнями** дисципліни є вивчення понять та теоретичних результатів сучасної криптографії, що використовуються при побудові захищених інформаційних систем в економіці, знайомство з основними моделями та методами захисту інформації.

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У результаті вивчення навчальної дисципліни «Кібербезпека фінансових систем» студенти мають набути таких результатів навчання та компетентностей :

Програмні компетентності	Програмні результати навчання
ЗК-03 Здатність до абстрактного мислення, аналізу та синтезу СК-16 Здатність розробляти та реалізовувати проекти інформаційних систем з використанням різних технологій проектування для здійснення інформаційно-аналітичної підтримки діяльності	ПРН-26 Розробляти та реалізовувати проекти інформаційних систем з використанням різних технологій проектування для здійснення аналітично-інформаційну підтримки діяльності суб'єктів господарювання.

¹ 1 змістовий модуль = 15 годин (0,5 кредита ECTS)



суб'єктів господарювання.	ПРН-28 Вміти розробляти й використовувати бази та сховища даних, призначених для вирішення економічних завдань, аналізу інформації та підготовки аналітичних звітів.
---------------------------	--

У разі успішного завершення курсу студент зможе:

- описувати криптографічні системи;
- застосовувати математичні моделі до криптографічних систем;
- розв'язувати задачі криптографічного шифрування даних;
- робити електронні підписи на документах;
- реалізувати основні етапи побудови математичної моделі безпеки інформаційної системи;
- проводити оцінку інформаційної безпеки підприємства, регіону, країни;
- вибирати відповідний метод захисту та застосовувати його;
- аналізувати ефективність системи безпеки інформації.

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

1. Фільштинський В. А., Бережний А. В. Математичні основи криптографії : конспект лекцій. Суми : Сумський державний університет, 2011. 138 с.
2. Остапов С. Е., Валь Л. О. Основи криптографії : навч. посіб. Чернівці : Книги-XXI, 2008. 188 с.
3. Козіна Г. Л., Молдов'ян М. А., Неласа Г. В. Криптопротоколи: схеми цифрового підпису : навч. посіб. Запоріжжя : ЗНТУ, 2014. 170 с.
4. Michael Braun and Anton Kargl. A Note on Signature Standards, 2007. URL: <http://eprint.iacr.org/2007/357>.
5. Матеріали, розміщені у системі Moodle на сторінці курсу за посиланням <https://moodle.znu.edu.ua/course/view.php?id=3029>.

КОНТРОЛЬНІ ЗАХОДИ

Поточні контрольні заходи (тах 60 балів):

Поточний контроль передбачає **теоретичні** завдання у вигляді тестування та опитувань за пройденим матеріалом у системі Moodle та **практичні** завдання у вигляді лабораторних робіт.

Тестування складається з запитань таких типів: вибір з відповідності, вибір з множини, вибір «так – ні». Тестування за кожним змістовим модулем складається з 6 запитань та оцінюється у **6 балів** кожне тестування, теоретичне опитування за темою – з 1 запитання та оцінюється у **1 бал**.

Лабораторна робота має бути оформлена у вигляді звіту, який складається з таких частин: назва лабораторної роботи; виконання лабораторної роботи, висновки. Оформлений звіт повинен бути поданий у системі Moodle. Повне виконання завдань лабораторних робіт оцінюється у **6 балів**.

Підсумкові контрольні заходи (тах 40 балів):

Підсумковий контроль складається з двох частин: теоретичної (**20 балів**) та практичної (**20 балів**).

Теоретична частина – тестування у системі Moodle. Максимальна оцінка, яку студент може отримати під час тестування, складає **20 балів**. Тестування за вивченим матеріалом курсу складається з 20 запитань наступних типів: вибір з відповідності, вибір з множини, вибір "так – ні". За кожну правильну відповідь студент отримує **1 бал**.

Також студент виконує індивідуальне практичне завдання (максимальна оцінка **10 балів**), а під час заліку виконує практичне завдання залікової роботи (письмово). Максимальна оцінка, яку

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЕКОНОМІЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни



студент може отримати за виконання практичного завдання, складає **10 балів**. Виконання студентом практичного завдання заліку оцінюються за такою шкалою:

10 балів – завдання виконано без помилок;

9-7 балів – завдання виконано з незначними помилками;

6-4 балів – завдання виконано з помилками (студент розуміє план розв'язання);

3-1 балів – студентом наведено формули для виконання завдання, але невірно їх застосовано;

0 балів – завдання не виконано.

Контрольний захід		Термін виконання	% від загальної оцінки
Поточний контроль (max 60%)			
Змістовий модуль 1	Вид теоретичного завдання: опитування за темою 1	тиждень 2	1%
	Вид практичного завдання: лабораторна робота 1	тиждень 2	5%
	Вид теоретичного завдання: опитування за темою 2	тиждень 4	2%
	Вид практичного завдання: лабораторна робота 2	тиждень 4	5%
	Вид практичного завдання: лабораторна робота 3	тиждень 4	5%
	Вид теоретичного завдання: тестування за змістовим модулем 1	тиждень 4	6%
Змістовий модуль 2	Вид теоретичного завдання: опитування за темою 3	тиждень 8	1%
	Вид практичного завдання: лабораторна робота 4	тиждень 8	5%
	Вид теоретичного завдання: тестування за змістовим модулем 2	тиждень 8	6%
Змістовий модуль 3	Вид теоретичного завдання: опитування за темою 5	тиждень 12	1%
	Вид практичного завдання: лабораторна робота 5	тиждень 12	5%
	Вид теоретичного завдання: тестування за змістовим модулем 3	тиждень 12	6%
Змістовий модуль 4	Вид теоретичного завдання: опитування за темою 7	тиждень 14	1%
	Вид практичного завдання: лабораторна робота 6	тиждень 14	5%
	Вид теоретичного завдання: тестування за змістовим модулем 4	тиждень 14	6%
Підсумковий контроль (max 40%)			
Підсумкове теоретичне завдання: тести у системі Moodle			20%
Підсумкове практичне завдання: виконання практичного завдання залікової роботи			20%
Разом			100%

Шкала оцінювання: національна та ECTS

За шкалою ECTS	За шкалою університету	За національною шкалою	
		Екзамен	Залік
A	90 – 100 (відмінно)	5 (відмінно)	Зараховано
B	85 – 89 (дуже добре)	4 (добре)	
C	75 – 84 (добре)		
D	70 – 74 (задовільно)	3 (задовільно)	
E	60 – 69 (достатньо)		

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЕКОНОМІЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни



FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)	Не зараховано
F	1 – 34 (незадовільно – з обов’язковим повторним курсом)		

РОЗКЛАД КУРСУ ЗА ТЕМАМИ І КОНТРОЛЬНІ ЗАВДАННЯ

Тиждень і вид заняття	Тема заняття	Контрольний захід	Кількість балів
Змістовий модуль 1			
Тиждень 1 Лекція 1	Тема 1. Класичні техніки шифрування		
Тиждень 2 Лабораторне заняття 1	Лабораторна робота 1. Класичні техніки шифрування	Опитування за темою 1	1
		Виконання та захист лабораторної роботи 1 (Класичні техніки шифрування)	5
Тиждень 3 Лекція 2	Тема 2. Математичні основи криптографії		
Тиждень 4 Лабораторне заняття 2	Лабораторна робота 2. Шифр Цезаря. Лабораторна робота 3. Афінна система шифрування Цезаря	Опитування за темою 2	2
		Виконання та захист лабораторної роботи 2	5
		Виконання та захист лабораторної роботи 3	5
		Тестування за змістовим модулем 1	6
Змістовий модуль 2			
Тиждень 5 Лекція 3	Тема 3. Основні принципи утворення криптографічних систем		
Тиждень 6 Лабораторне заняття 3	Лабораторна робота 4. Шифрувальна система на основі шифру гаммування	Виконання лабораторної роботи 4	
Тиждень 7 Лекція 4	Тема 4. Сучасні криптографічні системи		
Тиждень 8. Лабораторне заняття 4	Лабораторна робота 4. Шифрувальна система на основі шифру гаммування	Опитування за темою 3	1
		Виконання та захист лабораторної роботи 4	5
		Тестування за змістовим модулем 2	6
Змістовий модуль 3			
Тиждень 9 Лекція 5	Тема 5. Системи з відкритим ключем: асиметричні криптосистеми		



Тиждень 10. Лабораторне заняття 5	Лабораторна робота 5. Генерування ключів для системи шифрування RSA	Виконання лабораторної роботи 5	
Тиждень 11 Лекція 6	Тема 6. Цифровий електронний підпис		
Тиждень 12 Лабораторне заняття 6	Лабораторна робота 5. Генерування ключів для системи шифрування RSA	Опитування за темою 5	1
		Виконання та захист лабораторної роботи 5	5
		Тестування за змістовим модулем 3	6
Змістовий модуль 4			
Тиждень 13 Лекція 7	Тема 7. Місце криптографічних засобів захисту у загальному плані захисту інформації		
Тиждень 14 Лабораторне заняття 7	Лабораторна робота 6. Елементи криптоаналізу	Опитування за темою 7	1
		Виконання та захист лабораторної роботи 6	5
		Тестування за змістовим модулем 4	6

ОСНОВНІ ДЖЕРЕЛА

Книги:

1. Фільштінський В. А., Бережний А. В. Математичні основи криптографії : конспект лекцій. Суми : Сумський державний університет, 2011. 138 с.
2. Остапов С. Е., Валь Л. О. Основи криптографії : навч. посіб. Чернівці : Книги-XXI, 2008. 188 с.
3. Козіна Г. Л., Молдов'ян М. А., Неласа Г. В. Криптопротоколи: схеми цифрового підпису : навч. посіб. Запоріжжя : ЗНТУ, 2014. 170 с.
4. Michael Braun and Anton Kargl. A Note on Signature Standards, 2007. URL: <http://eprint.iacr.org/2007/357>.
5. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія. Харків : Вид. «Форт», 2010. 608 с.
6. Горбенко І. Д., Горбенко І. Д. Прикладна криптологія. Харків : Вид. «Форт», 2012. 878 с.
7. Кузнецов Г. В., Фомичов В. В., Сушко С. О., Фомичова Л.Я. Математичні основи криптографії. Дніпропетровськ : НГУ, 2006. 391 с.
8. Русин Б. П., Варецький Я. Ю. Біометрична аутентифікація та криптографічний захист : монографія. Львів : Коло, 2007. 287 с.
9. Задірака В. К., Олексюк О. С. Методи захисту фінансової інформації. Київ : Вища школа, 2009. 460 с.
10. Вербіцький О. В. Вступ до криптології. Львів : Науково-техн.літ., 1998. 248с.
11. Мухачев В. А., Хорошко В. А. Методы практической криптографии. Киев : ООО «Полиграф-Консалтинг», 2005. 215 с.
12. Ходаковський О. С. Криптографічний захист інформації. Рівне : МЕНУ, 2012. 108 с.



13. Задірака В. К., Кудін А. М., Людовиченко В. О., Олексюк О. С. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: навч. посіб. Київ – Тернопіль : Вид-во «Підручники і посібники», 2007. 272 с.
14. Бессалов А. В., Телиженко А. Б. Криптосистемы на эллиптических кривых: учеб. пособ. Киев : Политехника, 2004. 223 с.
15. Сушко С. О., Кузнецов Г. В., Фомичова Л. Я., Корабльов А. В. Математичні основи криптоаналізу: навч. посіб. для студ. вищ. навч. закл. : рек. МОНУ. Дніпропетровськ : НГУ, 2010. 466 с.

Законодавство України:

1. Про електронні довірчі послуги: Закон України № 2155-VIII від 5 жовтня 2017р. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#n534>.
2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України № 80/94-ВР від 5 липня 1994 р. URL: <https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>.
3. Про інформацію: Закон України № 2657-XII від 2 жовтня 1992 р. URL: <https://zakon3.rada.gov.ua/laws/show/2657-12>.
4. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ президента України № 505/98 від 22 травня 1998р. URL: <https://zakon.rada.gov.ua/laws/show/505/98>.

Інформаційні ресурси:

1. RSA Calculator. URL: <https://www.cs.drexel.edu/~jpoppyack/IntroCS/HW/RSAWorksheet.html>.
2. ITC Publishing. URL: <http://itc.ua>.
3. The International Association for Cryptologic Research (IACR). URL: <https://iacr.org>.
4. Useful Cryptography Resources – A Few Thoughts on Cryptographic Engineering/ URL: <https://blog.cryptographyengineering.com/useful-cryptography-resources>.
5. Best Cryptography Blogs and Websites. URL: <https://feedly.com/i/top/cryptography-blogs>.
6. 30 Best Cryptography Blogs & Websites. URL: https://blog.feedspot.com/cryptography_blogs.

7. Регуляції і політики курсу

Відвідування занять. Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу. Студент, який з поважних причин, підтверджених документально, був відсутній на практичному занятті, має право на відпрацювання після повернення до навчання. Якщо здобувач не використав надане йому право або пропустив заняття без поважних причин, отримує за кожне пропущене заняття 0 балів.

Академічна доброчесність. Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману. Неприпустиме складання роботи, виконаною іншою особою.

Використання комп'ютерів/телефонів на занятті. Використання подібних цифрових технічних засобів під час лекційних, практичних та лабораторних занять дозволяється виключно в навчальних цілях (з активованим режимом «без звуку»).

ДОДАТКОВА ІНФОРМАЦІЯ

ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ 2025/2026 н. р. доступний за адресою: <https://tinyurl.com/yckze4jd>.



ОСВІТНІЙ ПРОЦЕС ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ. Перевірка набутих студентами знань, навичок та вмінь (атестації, заліки, іспити та інші форми контролю) є невід'ємною складовою системи забезпечення якості освіти і проводиться відповідно до Положення про організацію та методику проведення поточного та підсумкового семестрового контролю навчання студентів ЗНУ: <https://tinyurl.com/y9tve4lk>.

ПОВТОРНЕ ВИВЧЕННЯ ДИСЦИПЛІН, ВІДРАХУВАННЯ. Наявність академічної заборгованості до 6 навчальних дисциплін (в тому числі проходження практики чи виконання курсової роботи) за результатами однієї екзаменаційної сесії є підставою для надання студенту права на повторне вивчення зазначених навчальних дисциплін. Порядок повторного вивчення визначається Положенням про порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ: <https://tinyurl.com/y9pkmmp5>. Підстави та процедури відрахування студентів, у тому числі за невиконання навчального плану, регламентуються Положенням про порядок переведення, відрахування та поновлення студентів у ЗНУ: <https://tinyurl.com/ycds57la>.

ВИРІШЕННЯ КОНФЛІКТІВ. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, регламентуються Положенням про порядок і процедури вирішення конфліктних ситуацій у ЗНУ: <https://tinyurl.com/57wha734>. Конфліктні ситуації, що виникають у сфері стипендіального забезпечення здобувачів вищої освіти, вирішуються стипендіальними комісіями факультетів, коледжів та університету в межах їх повноважень, відповідно до: Положення про порядок призначення і виплати академічних стипендій у ЗНУ: <https://tinyurl.com/yd6bq6p9>; Положення про призначення та виплату соціальних стипендій у ЗНУ: <https://tinyurl.com/y9r5dpwh>.

ПСИХОЛОГІЧНА ДОПОМОГА. Телефон довіри практичного психолога **Марті Ірини Вадимівни** (061) 228-15-84, (099) 253-78-73 (щоденно з 9 до 21).

УПОВНОВАЖЕНА ОСОБА З ПИТАНЬ ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ КОРУПЦІЇ
Запорізького національного університету: **Банах Віктор Аркадійович**
Електронна адреса: v_banakh@znu.edu.ua
Гаряча лінія: тел. (061) 227-12-76, факс 227-12-88

РІВНІ МОЖЛИВОСТІ ТА ІНКЛЮЗИВНЕ ОСВІТНЄ СЕРЕДОВИЩЕ. Центральні входи усіх навчальних корпусів ЗНУ обладнані пандусами для забезпечення доступу осіб з інвалідністю та інших маломобільних груп населення. Допомога для здійснення входу у разі потреби надається черговими охоронцями навчальних корпусів. Якщо вам потрібна спеціалізована допомога, будь ласка, зателефонуйте (061) 228-75-11 (начальник охорони). Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗНУ: <https://tinyurl.com/ydhcsagx>.

РЕСУРСИ ДЛЯ НАВЧАННЯ

НАУКОВА БІБЛІОТЕКА: <http://library.znu.edu.ua>. Графік роботи абонементів: понеділок-п'ятниця з 08.00 до 16.00; вихідні дні: субота і неділя.

СИСТЕМА ЕЛЕКТРОННОГО ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ (MOODLE):
<https://moodle.znu.edu.ua>

Якщо забули пароль/логін, направте листа з темою «Забув пароль/логін» за адресою: moodle.znu@znu.edu.ua.

У листі вкажіть: прізвище, ім'я, по-батькові українською мовою; шифр групи; електронну адресу.



Якщо ви вказували електронну адресу в профілі системи Moodle ЗНУ, то використовуйте посилання для відновлення паролю <https://moodle.znu.edu.ua/mod/page/view.php?id=133015>.

ЦЕНТР ІНТЕНСИВНОГО ВИВЧЕННЯ ІНОЗЕМНИХ МОВ: <http://sites.znu.edu.ua/child-advance/>

ЦЕНТР НІМЕЦЬКОЇ МОВИ, ПАРТНЕР ГЕТЕ-ІНСТИТУТУ:
<https://www.znu.edu.ua/ukr/edu/ocznu/nim>

ШКОЛА КОНФУЦІЯ (ВИВЧЕННЯ КИТАЙСЬКОЇ МОВИ): <http://sites.znu.edu.ua/confucius>