



«Інформаційна безпека: загрози та методи захисту»

Викладач: доктор фіз.-мат. Наук, професор, Козін Ігор Вікторович

Кафедра: економічної кібернетики, 5-й корпус ЗНУ, ауд.113

Е-mail: ainc@ukrpost.net

Телефон:

Інші засоби зв'язку:

Освітня програма, рівень вищої освіти	Економічна кібернетика бакалавр					
Статус дисципліни	Вибіркова					
Кредити ECTS 3		Навч. рік	2020-21	Рік навчання	Тижні	16
Кількість годин 90		Кількість змістових модулів ¹ 4		4-й	Лекційні заняття – 16 Лабораторні заняття – 16 Самостійна робота – 58	
Вид контролю	Залік					
Посилання на курс в Moodle [^]		https://moodle.znu.edu.ua/course/view.php?id=5616				
Консультації: 2 год на тиждень за розкладом		кількість на тиждень, тривалість, формат (за розкладом, за домовленістю, особисто чи дистанційно)				

ОПИС КУРСУ

Мета курсу.

Метою курсу «Інформаційна безпека: загрози та методи та захисту» є ознайомлення з сучасними методами захисту інформації і набуття теоретичних знань і практичних навичок з питань побудови ефективних інформаційних систем, моделей безпеки інформації, організації ефективного захисту інформації сучасними методами.

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У разі успішного завершення курсу студент **зможє:**

- 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;
- розв'язувати задачі криптографічного шифрування даних;
- робити електронні підписи на документах

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, плани семінарських занять, методичні рекомендації до виконання індивідуальних завдань розміщені на платформі Moodle:

<https://moodle.znu.edu.ua/course/view.php?id=5616>

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



КОНТРОЛЬНІ ЗАХОДИ

Поточні контрольні заходи:

Поточний контроль здійснюється у вигляді лабораторних робіт за темами та вигляді коротких тестувань (10 питань). Передбачено 8 лабораторних робіт, кожна з яких оцінюється в 6 балів та 2 тестових завдання по 6 балів. Тестування проводяться в системі Moodle.

Підсумкові контрольні заходи:

Підсумковий семестровий контроль складається з двох частин

1. Індивідуальне завдання за темами з заданого переліку тем. Максимальна оцінка – 20 балів
2. Підсумковий тест (Moodle) або опитування – Максимальна оцінка – 20 балів

Контрольний захід		Термін виконання	% від загальної оцінки	
Поточний контроль (max 60%)				
розділ 1	Змістовий модуль 1	Лабораторні роботи 1-2 Опитування	За розкладом занять	12
	Змістовий модуль 2	Лабораторна робота 3-4 Опитування Тестування	За розкладом занять	18
розділ 2	Змістовий модуль 3	Лабораторні роботи 5-6 Опитування	За розкладом занять	12
	Змістовий модуль 4	Лабораторна робота 7-8 Опитування Тестування	За розкладом занять	18
Підсумковий контроль (max 40%)				
Індивідуальне завдання				20
Підсумковий тест або/та опитування				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)		
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
-----------------------	--------------	-------------------	-----------------

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Економічний факультет
Силабус навчальної дисципліни



		Змістовий модуль 1	
Тиждень 1 Лекція 1 Лабораторна робота 1	Вступ. Предмет та задачі курсу. Основні визначення та термінологія. Література, що рекомендується..	Лабораторна робота 1	6
		Змістовий модуль 1	
Тиждень 2 Лекція 2 Лабораторна робота 2	Загрози безпеки та методи захисту. Основні шляхи витоку інформації та несанкціонованого доступу в каналах телекомунікацій.	Лабораторна робота 2	6
		Змістовий модуль 2	
Тиждень 3 Лекція 3 Лабораторна робота 3	Політика захисту інформації. Свідомість працівників. Окреслення небезпеки і потенційно можливих атак. Паролі. Firewall.	Лабораторна робота 3	6
		Змістовий модуль 2	
Тиждень 4 Лекція 4 Лабораторна робота 4	Організаційні методи захисту. Структура та задачі органів безпеки інформації в інформаційних системах	Тестування Лабораторна робота 4	12
		Змістовий модуль 3	
Тиждень 5 Лекція 5 Лабораторна робота 5	Криптографічний захист інформації. Основні принципи шифрування.	Лабораторна робота 5	6
		Змістовий модуль 3	
Тиждень 6 Лекція 6 Лабораторна робота 6	Криптографічні системи з закритим ключом. Односторонні функції. Хеш-функції.	Лабораторна робота 6	6
		Змістовий модуль 4	
Тиждень 7 Лекція 7 Лабораторна робота 7	Криптографічні системи з відкритим ключом. Стандарти шифрування. шифрування RSA	Лабораторна робота 7	6
		Змістовий модуль 4	
Тиждень 8 Лекція 8 Лабораторна робота 8	Електронний цифровий підпис. Протоколи цифрового підпису.	Тестування Лабораторна робота 8	12

ОСНОВНІ ДЖЕРЕЛА

Основна

1. Дж. Уолрэнд. Телекоммуникационные и компьютерные сети. Вводный курс. Москва: Постмаркет, 2001. – 480с.
2. Вербіцкий О.В. Вступ до криптології. – Видавництво наук.-техн. Літератури. Львів, 1998.
3. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов/ П.Н. Деревянин, О.О. Михальский, Д.И. Правиков и др. – М.: Радио и связь, 2000. – 192 с.



4. Коржик В.И., Кушнир Д.В. Теоретические основы информационной безопасности телекоммуникационных систем: учеб. пособие (спец. 200900, 201000, 060800)/ СПбГУТ. – СПб, 2000. – 134с.
5. Зегжда Д.П., Ивашко А.М. Основы информационной безопасности. – М.: Горячая линия - Телеком, 2000. – 452с.
6. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В., 2001, 352с.
7. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.
8. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, ПБОЮЛ Н.А. Егоров, 2001. – 264 с.
9. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «Безопасность». – М.: СИНТЕГ, 2000. - 248 с.
10. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.Ж КУДИЦ-ОБРАЗ, 2001 – 386с.

Додаткова література

1. Молдовян А.А., Молдовян Н.А., Советов А.Б. Криптография- Серия «Учебники для вузов. Специальная литература». – СПб.: Изд-во «Лань», 2000.- 224с.
2. Введение в криптографию / Под общ. Ред. В.В. Яценко. – 2-е изд., испр. – М.:МЦНМО: «ЧеРо», 1999. – 272с.
3. Нечаев В.И. Элементы криптографии (Основы теории защиты информации): Учеб. пособие для ун-тов и пед. вузов / Под ред. В.А.Садовниченко – М.: Высш.шк., 1999. – 109с.
4. Петраков А.В., Лагутин В.С. Утечка и защита информации в телефонных каналах. 3-е изд., исправл. и доп. – М.: Энергоатомиздат, 1998. – 320с.
5. М.Н. Аршинов, Л.Е. Садовский. Коды и математика (рассказы о кодировании).- М.: Наука, Главная редакция физико-математической литературы, 1983.- 144с. (Библиотечка «Квант». Выпуск 30).
6. Жельников В. Криптография от компьютера до папируса. – М., АБФ, 1997. – 336с.
7. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов/ П.Ю. Белкин, О.О.Михальский, А.С. Першаков и др. – М.: Радио и связь, 2000. – 168 с.
8. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов/ Проскурин В.Г., Крутов С.В., Маркевич И.В. – М.: Радио и связь, 2000. – 168 с.
9. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов/ П.Н. Деревянин, О.О.Михальский, Д.И. Правиков и др. – М.: Радио и связь, 2000. – 192 с.
10. Вербицкий О.В. Вступ до криптології. – Львів: ВНТЛ, 1998. – 248.
11. Журнал Захист інформації – Київ: Науково-технічний журнал. Засновано у 1999 році. Засновник - Київський міжнародний університет цивільної авіації.
12. Журнал Проблемы информационной безопасности. Компьютерные системы – С.-Петербург: Санкт-Петербургский государственный технический университет. Осн. в 1999г.
13. Журнал Безопасность информационных технологий – М.: Московский государственный технический университет.
14. Журнал Защита информации. Конфидент –С.-Пб:Информационно-методический журнал. Основан в 1994г., Изд. ООО «Конфидент».
15. Баричев С. Криптография без секретов.
16. Винокуров А. Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы Intel x86.// Монитор. М., 1995. №1,5.
17. Саломая А. Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995. – 318с.



18. Коржик В.И., Кушнир Д.В. Теоретические основы информационной безопасности телекоммуникационных систем: учеб. пособие (спец. 200900, 201000, 060800)/ СПбГУТ. – СПб, 2000. – 134с.

19. Зегжда Д.П., Ивашко А.М. Основы информационной безопасности. – М.: Горячая линия - Телеком, 2000. – 452с.

20. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В., 2001, 352с.

21. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.

22. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, ПБОЮЛ Н.А. Егоров, 2001. – 264 с.

23. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «Безопасность». – М.: СИНТЕГ, 2000. - 248 с.

24. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.Ж КУДИЦ-ОБРАЗ, 2001 – 386с.

25. Рассказ Эдгара По «Золотой жук».

26. Рассказ Артура Конан Дойля «Пляшущие человечки».

Інформаційні ресурси

1. RSA Calculator. URL: <https://www.cs.drexel.edu/~jpopuack/IntroCS/HW/RSAWorksheet.html>.

2. ITC Publishing. URL: <http://itc.ua>.

3. Криптография – шифрование и анализ / Хабр/. URL: <https://habr.com/hub/crypto>.

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ²

Відвідування занять. Регуляція пропусків.

Інтерактивний характер курсу передбачає обов'язкове відвідування практичних занять. Студенти, які за певних обставин не можуть відвідувати практичні заняття регулярно, мусять впродовж тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені завдання мають бути відпрацьовані на найближчій консультації впродовж тижня після пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання шляхом виконання індивідуального письмового завдання.

Студенти, які станом на початок екзаменаційної сесії мають понад 70% невідпрацьованих пропущених занять, до відпрацювання не допускаються.

Політика академічної доброчесності

Усі письмові роботи, що виконуються слухачами під час проходження курсу, перевіряються на наявність плагіату за допомогою спеціалізованого програмного забезпечення UniCheck. Відповідно до чинних правових норм, плагіатом вважатиметься: копіювання чужої наукової роботи чи декількох робіт та оприлюднення результату під своїм іменем; створення суміші власного та запозиченого тексту без належного цитування джерел; рерайт (перепарафразування чужої праці без згадування оригінального автора). Будь-яка ідея, думка чи речення, ілюстрація чи фото, яке ви запозичуєте, має супроводжуватися посиланням на першоджерело. Приклади оформлення цитувань див. на Moodle: <https://moodle.znu.edu.ua/mod/resource/view.php?id=103857>

² Тут зазначається все, що важливо для курсу: наприклад, умови допуску до лабораторій, реактивів тощо. Викладач сам вирішує, що треба знати студенту для успішного проходження курсу!



Виконавці індивідуальних дослідницьких завдань обов'язково додають до текстів своїх робіт власноруч підписану Декларацію академічної доброчесності (див. посилання у Додатку до силабусу).

Роботи, у яких виявлено ознаки плагіату, до розгляду не приймаються і відхиляються без права перекладання. Якщо ви не впевнені, чи підпадають зроблені вами запозичення під визначення плагіату, будь ласка, проконсультуйтеся з викладачем.

Висока академічна культура та європейські стандарти якості освіти, яких дотримуються у ЗНУ, вимагають від дослідників відповідального ставлення до вибору джерел. Посилання на такі ресурси, як Wikipedia, бази даних рефератів та письмових робіт (Studopedia.org та подібні) є неприпустимим. Рекомендовані бази даних для пошуку джерел:

Електронні ресурси Національної бібліотеки ім. Вернадського: <http://www.nbuv.gov.ua>

Цифрова повнотекстова база даних англomовної наукової періодики JSTOR: <https://www.jstor.org/>

Використання комп'ютерів/телефонів на занятті

Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). Будь ласка, не забувайте активувати режим «без звуку» до початку заняття.

Під час виконання заходів контролю (тестів, контрольних робіт, іспитів) використання гаджетів заборонено. У разі порушення цієї заборони роботу буде анульовано без права перекладання.

Комунікація

Базовою платформою для комунікації викладача зі студентами є Moodle.

Важливі повідомлення загального характеру – зокрема, оголошення про терміни подання контрольних робіт, коди доступу до сесій розміщуються викладачем на форумі курсу. Для персональних запитів використовується сервіс приватних повідомлень. Відповіді на запити студентів подаються викладачем впродовж тижня, або на чергові консультації.

Якщо за технічних причин доступ до Moodle є неможливим, або ваше питання потребує термінового розгляду, направте електронного листа з позначкою «Важливо» на адресу ainc@ukrpost.net. У листі обов'язково вкажіть ваше прізвище та ім'я, курс та шифр академічної групи.



ДОДАТОК ДО СИЛАБУСУ ЗНУ – 2020-2021 рр.

ГРАФІК НАВЧАЛЬНОГО ПРОЦЕСУ 2020-2021 н. р. (посилання на сторінку сайту ЗНУ)

АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ. Студенти і викладачі Запорізького національного університету несуть персональну відповідальність за дотримання принципів академічної доброчесності, затверджених **Кодексом академічної доброчесності ЗНУ**: <https://tinyurl.com/ya6yk4ad>. Декларація академічної доброчесності здобувача вищої освіти (додається в обов'язковому порядку до письмових кваліфікаційних робіт, виконаних здобувачем, та засвідчується особистим підписом): <https://tinyurl.com/y6wzzlu3>.

НАВЧАЛЬНИЙ 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 методу 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>.

НЕФОРМАЛЬНА ОСВІТА. Порядок зарахування результатів навчання, підтверджених сертифікатами, свідоцтвами, іншими документами, здобутими поза основним місцем навчання, регулюється *Положенням про порядок визнання результатів навчання, отриманих у неформальній освіті*: <https://tinyurl.com/y8gbt4xs>.

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/ycyfws9v>. 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 (061)228-15-84 (щоденно з 9 до 21).

ЗАПОБІГАННЯ КОРУПЦІЇ. Уповноважена особа з питань запобігання та виявлення корупції (Воронков В. В., 1 корп., 29 каб., тел. +38 (061) 289-14-18).

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 17.00; субота з 09.00 до 15.00.

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

Якщо забули пароль/логін, направте листа з темою «Забув пароль/логін» за адресами:

- для студентів ЗНУ - moodle.znu@gmail.com, Савченко Тетяна Володимирівна
- для студентів Інженерного інституту ЗНУ - alexvask54@gmail.com, Василенко Олексій Володимирович

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/ocnu/nim>

Школа Конфуція (вивчення китайської мови): <http://sites.znu.edu.ua/confucius>