ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ і ТЕХНОЛОГІЙ

STATE UNIVERSITY OF ECONOMICS AND TECHNOLOGY
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТЕХНОЛОГІЙ

SYLLABUS / РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Course of study (code) / Назва дисципліни (шифр)	ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ EI1224BOIMB
Academic year / Навчальний рік - Семестр	**2022/2023–7 семестр**
Course of study / Назва спеціальності	**122 Комп'ютерні науки**
Educational program / Освітня програма **Education - ECTS / Рівень – Кредити** **Status / Статус** **Learning language / Мова навчання**	**Комп'ютерні науки** **Перший (бакалаврський) рівень – 4 ECTS** **Обов'язкова** **Українська**
Author / Укладач	**Соловйова Вікторія Володимирівна, кандидат економічних наук, доцент,** **Державний університет економіки і технологій,** **e-mail: solovieva_vv@kneu.dp.ua,** **https://orcid.org/ 0000-0002-8090-9569,** **моб. +380972698959**
Консультації	**Чт. 15.00-16.00**

A. OBJECTIVE OF THE SUBJECT / МЕТА ТА ЗАВДАННЯ ДИСЦИПЛІНИ

Метою викладання дисципліни є формування теоретичних знань та практичних навичок, необхідних для створення умов, що запобігають розголошенню, витоку і неправомірному оволодінню конфіденційною інформацією, а також запобігають протиправним діям щодо знищення, модифікації, копіювання і блокування інформації.

Завдання вивчення дисципліни є у тому, щоб ознайомити студентів із законодавчим, адміністративним, організаційним і інженерно-технічним рівнями забезпечення інформаційної безпеки, особливостями криптографічного і стенографічного захисту інформації, навчити їх реалізовувати практично правила політики безпеки підприємства.

B. SUBJECT PROGRAM / ПРОГРАМА ДИСЦИПЛІНИ

1. Поняття інформаційної безпеки. Основні задачі інформаційної безпеки. Важливість і складність проблеми інформаційної безпеки. Основні концептуальні положення системи захисту інформації. Поняття системи захисту інформації. Вимоги до захисту інформації. Вимоги до системи захисту інформації. Види забезпечення системи захисту інформації.
2. Основні загрози безпеки. Загальні відомості. Основні ненавмисні штучні загрози. Основні навмисні штучні загрози. Класифікація загроз безпеки. Опис моделі гіпотетичного порушника. Види інформації, що захищається в сфері управління. Контроль якості інформації.
3. Стандарти та специфікації в галузі інформаційної безпеки. Основні поняття та історія. Нормативна база. Канадські критерії оцінки безпеки надійних комп'ютерних систем. Федеральні критерії. Єдині критерії оцінки безпеки інформаційних технологій, iso / iec 15408. «Помаранчева» книга». Українські критерії оцінки.
4. Адміністративний рівень забезпечення інформаційної безпеки. Цілі, завдання і зміст адміністративного рівня. Розробка політики інформаційної безпеки. Політика безпеки верхнього рівня. Політика безпеки середнього рівня. Політика безпеки нижнього рівня. Програма безпеки. Управління ризиками.
5. Загрози та головні уразливості критично-важливих об'єктів інфраструктури. Передумови появи, природа походження та джерела загроз. Основні методи та способи реалізації загроз. Способи реалізації загроз. Модель загроз та модель порушника. Еволюція тактики та таксономії реалізації загроз. Систематизація (класифікація) та зміна ландшафту загроз безпеці ІТС. Класифікація загроз за видами ознак. Класифікація загроз за видами діяльності. Каталогізація загроз та їх головні аспекти. Типи загроз безпеці інформації в ІТС. Перелік можливих загроз IP, що циркулює та обробляється в ІТС. Загальний порядок виявлення актуальних загроз для ІТС. Загальна схема і алгоритм оцінювання загроз ІТС. Методи експертного оцінювання загроз ІТС. Шляхи мінімізації внутрішніх і зовнішніх загроз. Статистика вразливостей ОС, ПЗ і додатків.
6. Інженерно-технічний рівень інформаційної безпеки. Поняття інженерно-технічного захисту. Фізичні засоби захисту. Види фізичних засобів. Захист інформації від витоку по технічним каналам. Протидії несанкціонованому доступу до джерел конфіденційної інформації. Апаратні засоби захисту. Програмні засоби захисту.
7. Криптографічний захист інформації. Поняття систем криптографічного захисту. Криптосистеми з секретним ключем. Криптосистеми з відкритим ключем. Архівування з шифруванням. Шифрування дисків.
8. Захист програм. Актуальні задачі захисту програм. Реєстраційні коди для програм. Прив'язка програм до носіїв інформації. Апаратні ключі захисту програм. Захист від шкідливого програмного забезпечення. Цілі захисту. Визначення видів захисту від вірусів. Правила експлуатації стороннього програмного забезпечення. Залучення користувачів до захисту від вірусів.

C. LIST OF COMPETENCIES AND STUDIES TARGETED RESULTS / ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ТА ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ

Загальні компетентності (ЗК)	ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК6. Здатність вчитися й оволодівати сучасними знаннями. ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК8. Здатність генерувати нові ідеї (креативність). ЗК10. Здатність бути критичним і самокритичним. ЗК11. Здатність приймати обґрунтовані рішення. ЗК13. Здатність діяти на основі етичних міркувань. ЗК14. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗК15. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Спеціальні (фахові) компетентності (ФК)	СК4. Здатність використовувати сучасні методи математичного моделювання об'єктів, процесів і явищ, розробляти моделі й алгоритми чисельного розв'язування задач математичного моделювання, враховувати похибки наближеного чисельного розв'язування професійних задач. СК6. Здатність до системного мислення, застосування методології системного аналізу для дослідження складних проблем різної природи, методів формалізації та розв'язування системних задач, що мають суперечливі цілі, невизначеності та ризики. СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.
Програмні результати навчання (ПРН)	ПР1. Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук. ПР16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

D. SEMESTER PLAN / СЕМЕСТРОВИЙ ПЛАН

Тиждень/ Дата	Тема, план/короткі тези	Форма діяльності (заняття), години, формат	Завдання для СРС (література, ресурси в інтернеті, презентація, відеокурси)
Згідно розкладу	*Тема 1.* Основні положення інформаційної безпеки. Поняття інформаційної безпеки. Основні задачі інформаційної безпеки. Важливість і складність проблеми інформаційної безпеки. Основні концептуальні положення системи захисту інформації.	лекція (2 год.,), F2F Лабораторна робота (4 год.)	Опрацювання літератури: основна 1 - 5 додаткова 1 – 16

	Поняття системи захисту інформації. Вимоги до захисту інформації. Вимоги до системи захисту інформації. Види забезпечення системи захисту інформації. *Тема 2.* Основні загрози безпеки. Основні ненавмисні штучні загрози. Основні навмисні штучні загрози. Класифікація загроз безпеки. Опис моделі гіпотетичного порушника. Види інформації, що захищається в сфері управління. Контроль якості інформації. *Тема 3.* Стандарти та специфікації в галузі інформаційної безпеки. Основні поняття та історія. Нормативна база. Канадські критерії оцінки безпеки надійних комп'ютерних систем. Федеральні критерії. Єдині критерії оцінки безпеки інформаційних технологій, iso / iec 15408. «Помаранчева» книга». Українські критерії оцінки. *Тема 4.* Адміністративний рівень забезпечення інформаційної безпеки. Цілі, завдання і зміст адміністративного рівня. Розробка політики інформаційної безпеки. Політика безпеки верхнього рівня. Політика безпеки середнього рівня. Політика безпеки нижнього рівня. Програма безпеки. Управління ризиками. *Тема 5.* Загрози та головні уразливості критично-важливих об'єктів інфраструктури Передумови появи, природа походження та джерела загроз. Основні методи та способи реалізації загроз. Способи реалізації загроз. Модель загроз та модель порушника. Еволюція тактики та таксономії реалізації загроз. Систематизація (класифікація) та зміна ландшафту загроз безпеці ІТС. Класифікація загроз за видами ознак. Класифікація загроз за видами діяльності. Каталогізація загроз та їх головні аспекти. Типи загроз безпеці	лекція (2 год.,), F2F Лабораторна робота (4 год.) лекція (2 год.,), F2F Лабораторна робота (4 год.) лекція (2 год.,), F2F Лабораторна робота (4 год.) лекція (2 год.,), F2F Лабораторна робота (4 год.)	Опрацювання літератури: основна 1 - 5 додаткова 1 - 16 Опрацювання літератури: основна 1 - 5 додаткова 1 - 16 Опрацювання літератури: основна 1 - 5 додаткова 1 – 16 Опрацювання літератури: основна 1 - 5 додаткова 1 – 16

	інформації в ІТС. Перелік можливих загроз ІР, що циркулює та обробляється в ІТС. Загальний порядок виявлення актуальних загроз для ІТС. Загальна схема і алгоритм оцінювання загроз ІТС. Методи експертного оцінювання загроз ІТС. Шляхи мінімізації внутрішніх і зовнішніх загроз. Статистика уразливостей ОС, ПЗ і додатків.		Опрацювання літератури: основна 1 - 5 додаткова 1 – 16
	Тема 6. Інженерно-технічний рівень інформаційної безпеки. Поняття інженерно-технічного захисту. Фізичні засоби захисту. Види фізичних засобів. Захист інформації від витоку по технічним каналам. Протидії несанкціонованому доступу до джерел конфіденційної інформації. Апаратні засоби захисту. Програмні засоби захисту.	лекція (2 год.,), F2F Лабораторна робота (4 год.)	Опрацювання літератури: основна 1 - 5 додаткова 1 – 6
	Тема 7. Криптографічний захист інформації. Поняття систем криптографічного захисту. Криптосистеми з секретним ключем. Криптосистеми з відкритим ключем. Архівування з шифруванням. Шифрування дисків.	лекція (2 год.,), F2F Лабораторна робота (4 год.)	Опрацювання літератури: основна 1 - 5 додаткова 1 – 16
	Тема 8. Захист програм. Актуальні задачі захисту програм. Реєстраційні коди для програм. Прив'язка програм до носіїв інформації. Апаратні ключі захисту програм. Захист від шкідливого програмного забезпечення. Цілі захисту. Визначення видів захисту від вірусів. Правила експлуатації стороннього програмного забезпечення. Залучення користувачів до захисту від вірусів.	лекція (2 год.,), F2F Лабораторна робота (4 год.)	Опрацювання літератури: основна 1 - 5 додаткова 1 - 16

E. BASIC LITERATURE (OBLIGATORY TEXTBOOKS) / ОСНОВНА ЛІТЕРАТУРА (ОБОВ'ЯЗКОВІ ПІДРУЧНИКИ)

1. Основи інформаційної безпеки : Навчальний посібник / В.А. Лужецький, А.Д. Кожухівський, О.П. Войтович. – Вінниця : ВНТУ, 2013. – 221 с.
2. Рибальський О.В., Смаглюк В.М., Хахановський В.Г. Основи інформаційної безпеки. Пі-дручник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2010. – 255 с.
3. Бармен, Скотт. Разработка правил информационной безопасности.: Пер. с англ.— М.: Издательский дом «Вильяме», 2002.— 208 с.
4. Домарев В.В. Безопасность информационных технологий. Системный подход.- К.: ООО «ТИД «ДС», 2004.- 992 с.
5. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

F. COMPLEMENTARY LITERATURE / ДОДАТКОВА ЛІТЕРАТУРА

1. Закон України «Про інформацію» : за станом на 1 січня 2013 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»: за станом на 1 січня 2013 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgibin/laws/main.cgi?nreg=80%2F94-%E2%F0
3. Нормативные акты Украины // www.nau.kiev.ua
4. Пошукова система у базі лекцій, наукових статей, навчальних посібників та підручників з усього світу/Google Академія - Режим доступу до ресурсу: http://scholar.google.com.ua/
5. Журнал "Информационные технологии. Аналитические материалы". – http://it.ridne.net
6. Центр информационных технологий. – http://www.citmgu.ru 4. Історія розвитку інформаційних технологій в Україні. – http://www.icfcst.kiev.ua/MUSEUM/IT_u.html
7. http://bezopasnost.biz.
8. http://dstszi.gov.ua.
9. www.fbi.gov.
10. www.pgpi.org.
11. www.rootshell.com.
12. www.securityfocus.com.
13. www.sysinternals.com.
14. www.zdnet.ru.
15. www.submarine.ru.
16. www.securitylab.ru.

G. THE MOST IMPORTANT PUBLICATIONS OF THE AUTHOR(S) CONCERNING PROPOSED CLASSES / ОСНОВНІ ПУБЛІКАЦІЇ АВТОРА, ЩО ПОВЯЗАНІ З ТЕМАТИКОЮ ЗАПЛАНОВАНИХ ЗАНЯТЬ

1.Victoria Solovieva, Sergiy Tkalichenko, Valentyna Khotskina. Cybercrime: the comparative analysis of the modern information space // INTERNATIONAL SCIENTIFIC JOURNAL «COMPUTER SYSTEMS AND INFORMATION TECHNOLOGIES», 2021, No 1 56-62 DOI: 10.31891/CSIT-2021-3-8 Фахова реєстрація **(категорія «Б»)**
2. Victoria Solovieva, Sergiy Tkalichenko, Valentyna Khotskina1, Zhanna Tsymbal, and Olena Burunova. Modern Structural Level and Dynamics of Crimes with The Use of Computers, Automation Systems, Computer Networks and Electric Connection Systems. SHS Web of Conferences 100, 01014 (2021) https://doi.org/10.1051/shsconf/202110001014 ISCSAI 2021**. (Web of Science Core Collection)**

H. PREREQUISITE AND POSTREQUISITE / ПРЕРЕКВІЗИТИ ТА ПОСТРЕКВІЗИТИ

I. SCOPE AND TYPE / КІЛЬКІСТЬ ВІДВЕДЕНИХ ГОДИН ТА ФОРМА ПРОВЕДЕННЯ ЗАНЯТЬ

	Денна	Заочна
Лекції	16	8
Практичні (лабораторні)	32	8
Самостійна робота студента (СРС)	64	88
Індивідуально-консультативна робота (ІКР)	8	16
Курсова робота	-	-
Разом годин	**120**	**120**

J. CURRENT AND FINAL EVALUATION / ПОТОЧНЕ ТА ПІДСУМКОВЕ ОЦІНЮВАННЯ

	Денна	Заочна
Поточний контроль, в т.ч.:	50	50
оцінювання під час аудиторних занять	10	5
виконання контрольних (модульних) робіт	10	10
виконання і захист завдань самостійної роботи	25	25
науково-дослідницька робота	5	10
Підсумковий контроль (екзамен)	50	50
Разом	100	100

Шкала балів	Оцінка за 4-бальноюшкалою	Шкала ECTS
90 – 100	Відмінно	A
80 – 89	Добре	B
70 – 79		C
66 – 69	Задовільно	D
60 – 65		E
21 – 59	незадовільно з можливістю повторного складання екзамену (заліку)	FX
0 – 20	незадовільно з можливістю вивчення дисципліни за індивідуальним графіком у формі додаткової індивідуально-консультативної роботи	F

K. CODE OF CONDUCT OF THE COURSE / КОДЕКС ПОВЕДІНКИ ПІД ЧАС ВИВЧЕННЯ КУРСУ

Для успішного проходження курсу та складання контрольних заходів необхідним є виконання наступних обов'язків:

- не запізнюватися на заняття;
- не пропускати заняття (як лекційні. так і практичні), в разі хвороби мати довідку або її ксерокопію;
- самостійно опрацьовувати весь лекційний матеріал та ресурси для самостійної роботи;
- конструктивно підтримувати зворотній зв'язок з викладачем на всіх етапах проходження курсу;
- своєчасно і самостійно виконувати всі передбачені програмою лабораторні та практичні завдання;

брати очну участь у контрольних заходах.

L. METHODS OF CONDUCTING / МЕТОДИ НАВЧАННЯ

Для формувань уміння та навичок застосовуються такі методи навчання:

- вербальні/словесні (лекція, пояснення, розповідь, бесіда, інструктаж);
- наочні (спостереження, ілюстрація, демонстрація);
- практичні (різні види вправляння, виконання графічних робіт, проведення експерименту, практики);
- пояснювально-ілюстративний або інформаційно-рецептивний, який передбачає пред'явлення готової інформації викладачем та її засвоєння студентами;
- репродуктивний, в основу якого покладено виконання різного роду завдань за зразком;
- метод проблемного викладу.
- частково-пошуковий або евристичний.
- Дослідницький.

M. TOOLS, EQUIPMENT AND SOFTWARE / ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

мультимедійний клас з ПК, цифровий проектор

Zoom – хмарна платформа для відео і аудіо конференцій та вебінарів.

Telegram – програма мессенжер.

viber – програма для відео та голосового зв'язку.

ZELIS - система призначена для тестування знань студентів в двох режимах: автоматизований контроль знань та тестування по бланкам.

N. STUDENT RESOURCES, MOOC PLATFORMS / ЦИФРОВІ РЕСУРСИ ДЛЯ СТУДЕНТІВ ТА ВІДКРИТІ ДИСТАНЦІЙНІ ОНЛАЙН КУРСИ

Студентам пропонується доступ до навчальних матеріалів дисципліни - moodle.kneu.dp.ua:

Coursera – безкоштовні онлайн-курси з різних дисциплін, у разі успішного закінчення яких користувач отримує сертифікат про проходження курсу.

EdX – онлайн-курси від закладів вищої освіти.

Prometheus — український громадський проєкт масових відкритих онлайн-курсів.

O. FEEDBACK/ ЗВОРОТНІЙ ЗВ'ЯЗОК

Електронні листи є найкращим способом зв'язатися з керівником курсу, і, будь ласка, додайте шифр групи в темі листа. Якщо ви надішлете мені електронне повідомлення, надайте мені, принаймні, 24 години, щоб відповісти. Якщо ви не отримаєте відповідь, відправте листа повторно.

P. ACADEMIC HONESTY/ АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ

Державний університет економіки і технологій очікує від студентів розуміння та підтримання високих стандартів академічної чесності. Приклади академічної не доброчесності включають такі: плагіат, зловживання інформацією із застарілих джерел мережі. Очікується, що вся робота, виконана відповідно до

вимог курсу, є власною роботою студента. Під час підготовки роботи, яка відповідає вимогам курсу, студенти повинні відрізняти власні ідеї від інформації, отриманої з інших джерел. Без попереднього письмового схвалення викладачем, студенти можуть не подавати один і той же звіт двічі.
Обов'язково вказати на положення про доброчесність й зробити гіперпосилання на сайт Університету (Положення про академічну доброчесність у Державному університеті економіки і технологій. Затверджено Вченою радою Державного університету економіки і технологій, Протокол № 5 від 25 листопада 2021 р.)
https://www.duet.edu.ua/uploads/normbase/243/pol_AD.pdf

APPROVED / ЗАТВЕРДЖЕНО

Рішенням кафедри «Економіки та цифрового бізнесу» Державного університету економіки і технологій - протокол № _1_ від 05__.10__.2022 року

Укладач — Вікторія СОЛОВЙОВА

ЗАТВЕРДЖЕНО:
Кафедрою економіки та цифрового бізнесу
Протокол № _1_ від _05_ __жовтня__ 2022 року
В.о. завідувача кафедри — Вікторія СОЛОВЙОВА

Науково-методичною радою Державного університету економіки і технологій
Протокол № _4_ від 30_ _листопада_ 2022 року
Голова науково-методичної ради — Валентин ОРЛОВ