



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет управління фінансами та бізнесу
Кафедра цифрової економіки та бізнес-аналітики

ЗАТВЕРДЖЕНО

На засіданні кафедри цифрової економіки та
бізнес-аналітики
факультету управління фінансами та бізнесу
Львівського національного університету
імені Івана Франка
(протокол № 1 від 27 серпня 2025 р.)

Завідувач кафедри  Ірина ШЕВЧУК

Силабус з навчальної дисципліни
«Захист інформації в інформаційних системах»,
що викладається в межах ОПП
«Інформаційні технології в бізнесі»
першого (бакалаврського) рівня вищої освіти для здобувачів
зі спеціальності 051 «Економіка»

Львів 2025 р.

Назва дисципліни	ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ
Адреса викладання дисципліни	м. Львів, вул. Коперника, 3
Факультет та кафедра, за якою закріплена дисципліна	Факультет управління фінансами та бізнесу Кафедра цифрової економіки та бізнес-аналітики
Галузь знань, шифр та назва спеціальності	05 «Соціальна та поведінкові науки» 051 «Економіка»
Викладачі дисципліни	Задорожна Анна Володимирівна, к.ф.-м.н., доцент, доцент кафедри цифрової економіки та бізнес-аналітики
Контактна інформація викладачів	anna.zadorozhna@lnu.edu.ua Сторінка викладача: https://financial.lnu.edu.ua/employee/zadorozhna-anna-volodymyrivna Місце знаходження: м. Львів, вул. Коперника, 3; кім. 508 (кафедра цифрової економіки та бізнес-аналітики)
Консультації з питань навчання по дисципліні відбуваються	Консультації відбуваються у день проведення лекцій/лабораторних занять, а також за попередньою домовленістю. Можливі он-лайн консультації через платформу Microsoft Teams.
Сторінка курсу	https://financial.lnu.edu.ua/course/zakhyst-informatsii-v-informatsiynykh-systemakh Платформа MOODLE: http://e-learning.lnu.edu.ua/login/index.php
Інформація про дисципліну	Дисципліна «Захист інформації в інформаційних системах» є нормативною дисципліною зі спеціальності 051 «Економіка» для освітньої програми «Інформаційні технології в бізнесі», яка викладається у VIII семестрі в обсязі 3 кредити (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Навчальна дисципліна «Захист інформації в інформаційних системах» спрямована на формування системних знань і практичних навичок у сфері захисту інформації та безпечного функціонування інформаційних систем. Курс забезпечує здатність здобувачів застосовувати сучасні методи і засоби забезпечення інформаційної безпеки, оцінювати ризики та впроваджувати заходи для захисту інформаційних ресурсів. У процесі навчання приділяється увага розвитку практичних умінь і компетентностей, необхідних для забезпечення конфіденційності, цілісності та доступності інформації в різних цифрових середовищах.
Мета та цілі дисципліни	Метою вивчення нормативної дисципліни «Захист інформації в інформаційних системах» є формування у здобувачів системних теоретичних знань і практичних навичок щодо забезпечення захисту інформації, оцінювання ризиків і застосування сучасних методів і засобів інформаційної безпеки в інформаційних системах. Основні завдання дисципліни «Захист інформації в інформаційних системах» – вивчення сучасних інформаційних технологій у галузі інформаційної безпеки та криптографічних методів захисту інформації;

	<p>підготовка фахівців із розробки та впровадження технологій комп'ютерного захисту інформації; забезпечення цілісності даних і конфіденційності; контроль передачі інформації, ідентифікація та автентифікація користувачів; застосування криптографії та інтегрованих систем захисту; формування політики безпеки та менеджменту в галузі інформаційної безпеки.</p>
<p>Література для вивчення дисципліни</p>	<p>Література:</p> <p>Основна:</p> <ol style="list-style-type: none"> 1. Задорожна, А. Кіберризика та страхування ІТ-відповідальності: міжнародний та вітчизняний досвід. <i>Фінансовий простір</i>. 2025, № 4 (58). С. 71-82. DOI: https://doi.org/10.30970/fr.4(58).2025.718182 2. Інформаційні технології в бізнесі. Частина 1: Навч. посіб. / [Шевчук І. Б., Старух А. І., Васьків О. М. та ін.]; за заг. ред. І. Б. Шевчук. Львів: Видавництво ННВК «АТБ», 2020. – 535 с. 3. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навч. посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с. 4. Костюк Ю. В. Системи захисту інформації : підручник / Ю. В. Костюк, П. М. Складанний, Г. М. Гулак, Б. Т. Бебешко, К. В. Хорольська, С. Л. Рзаєва. – Київ : Київський столичний університет імені Бориса Грінченка, 2025. – 887 с. URL : https://elibrary.kubg.edu.ua/id/eprint/51359/1/Kostiuk_Y_Skladannyi_P_Hulak_H_Bebeshko_V_Khorolska_K_Rzaieva_S_SZI_2025_FITM.pdf 5. Лісовська Ю. Інформаційна безпека України. Київ : Кондор, 2024. 320 с. 6. Остроухов В. В., Присяжнюк М. М., Фармагей О. І. Інформаційна безпека: підручник. – К. : Кондор, 2021. – 412 с. URL : https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf?srsltid=AfmBOopsSZ1H1VS6oFrFeaFo_dtzSltnDjysJZ8MO8xGXGCPtesvtCB8& 7. Пашорін В. І., Костюк Ю. В. Безпека інформаційних систем : навч. посіб. Львів : ФОП Марченко Т.В., 2025. – 376 с. 8. Смірнов О. А., Коноплицька-Слободенюк О. К., Смірнов С. А., Буравченко К. О., Смірнова Т. В., Поліщук Л. І. Інформаційна безпека в комп'ютерних мережах : навч. посіб. – Кропивницький : Видавець Лисенко В. Ф., 2020. – 295 с. URL : https://www.duikt.edu.ua/uploads/1_1487_78606346.pdf 9. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с. URL : https://ela.kpi.ua/bitstream/123456789/45723/1/NP_TZI_ITS.pdf 10. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с. 11. Zadorozhna A. Digital technologies as a factor of nationality security of Ukraine. <i>Vadyba Journal of Management</i>. 2023, Vol. 39, No. 2. P. 23–29. URL : https://doi.org/10.38104/vadyba.2023.2.03 <p>Додаткова:</p> <ol style="list-style-type: none"> 1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. URL : https://zakon.rada.gov.ua/laws/show/2657-12 2. Закон України «Про захист інформації в інформаційно-

	<p>комунікаційних системах» від 05.07.1994 № 80/94-ВР. URL : https://zakon.rada.gov.ua/laws/show/80/94-вр</p> <p>3. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19</p> <p>4. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII. URL : https://zakon.rada.gov.ua/laws/show/2155-19</p> <p>5. Технології захисту локальних мереж на основі обладнання CISCO: навч. посіб. /Т. І. Коробейнікова, С. М. Захарченко. – Львів : Видавництво Львівська політехніка, 2021. – 232 с.</p> <p>6. Easttom W. Modern Cryptography: Applied Mathematics for Encryption and Information Security / Springer International Publishing AG., 2022. xxiv, 453 p.</p> <p>7. Thakur K., Pathan A. K. Cybersecurity Fundamentals: A Real-World Perspective / CRC Press (Taylor & Francis Group), 2020. – 304 p.</p> <p>8. Chauhan S. R., Jangra S. Computer Security and Encryption / Mercury Learning and Information, 2020. 320 p.</p> <p>Інтернет-ресурси:</p> <p>1. Сайт журналу «Безпека інформації». URL: https://jrnl.nau.edu.ua/index.php/Infosecurity</p> <p>2. The CrypTool Portal. URL : https://www.cryptool.org/en</p> <p>3. ENISA – European Union Agency for Cybersecurity — аналітика, кращі практики та рекомендації з кібербезпеки, управління ризиками та захисту даних. URL : https://www.enisa.europa.eu/</p> <p>4. NIST. URL: https://csrc.nist.gov/</p>
Тривалість курсу	90 год.
Обсяг курсу	<p>Загальний обсяг (денна форма навчання): 90 год. (3 кредити ЄКТС). Аудиторна робота – 54 год., з них:</p> <ul style="list-style-type: none"> • лекції – 16 год.; • лабораторні заняття – 36 год. <p>Самостійна робота – 36 год.</p>
Компетентності та програмні результати навчання	<p>При вивченні дисципліни «Захист інформації в інформаційних системах» здобувачі вищої освіти набувають такі компетентності (здатність):</p> <p>ІК1 – Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми в економічній сфері, які характеризуються комплексністю та невизначеністю умов, що передбачає застосування теорій та методів економічної науки.</p> <p>ЗК3 – Здатність до абстрактного мислення, аналізу та синтезу.</p> <p>ЗК4 – Здатність застосовувати знання у практичних ситуаціях.</p> <p>ЗК7 – Навички використання інформаційних і комунікаційних технологій.</p> <p>ЗК9 – Здатність до адаптації та дій в новій ситуації.</p> <p>ЗК11 – Здатність приймати обґрунтовані рішення.</p> <p>СК2 – Здатність здійснювати професійну діяльність у відповідності з чинними нормативними та правовими актами.</p> <p>СК7 – Здатність застосовувати комп’ютерні технології та програмне забезпечення з обробки даних для вирішення економічних завдань, аналізу інформації та підготовки аналітичних звітів.</p> <p>СК12 – Здатність самостійно виявляти проблеми економічного характеру при аналізі конкретних ситуацій, пропонувати способи їх</p>

вирішення.

СК14 – Здатність поглиблено аналізувати проблеми і явища в одній або декількох професійних сферах з врахуванням економічних ризиків та можливих соціально-економічних наслідків.

СК16 – Здатність до аналізу, синтезу й оптимізації інформаційних систем та технологій з використанням математичних моделей і методів.

СК17 – Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями.

Програмні результати навчання:

ПР01 – Асоціювати себе як члена громадянського суспільства, наукової спільноти, визнавати верховенство права, зокрема у професійній діяльності, розуміти і вміти користуватися власними правами і свободами, виявляти повагу до прав і свобод інших осіб, зокрема, членів колективу.

ПР05 – Застосовувати аналітичний та методичний інструментарій для обґрунтування пропозицій та прийняття управлінських рішень різними економічними агентами (індивідуумами, домогосподарствами, підприємствами та органами державної влади).

ПР06 – Використовувати професійну аргументацію для донесення інформації, ідей, проблем та способів їх вирішення до фахівців і нефахівців у сфері економічної діяльності.

ПР10 – Проводити аналіз функціонування та розвитку суб'єктів господарювання, визначати функціональні сфери, розраховувати відповідні показники які характеризують результативність їх діяльності.

ПР12 – Застосовувати набуті теоретичні знання для розв'язання практичних завдань та змістовно інтерпретувати отримані результати.

ПР13 – Ідентифікувати джерела та розуміти методологію визначення і методи отримання соціально-економічних даних, збирати та аналізувати необхідну інформацію, розраховувати економічні та соціальні показники.

ПР14 – Визначати та планувати можливості особистого професійного розвитку.

ПР16 – Вміти використовувати дані, надавати аргументацію, критично оцінювати логіку та формувати висновки з наукових та аналітичних текстів з економіки.

ПР18 – Використовувати нормативні та правові акти, що регламентують професійну діяльність.

ПР19 – Використовувати інформаційні та комунікаційні технології для вирішення соціально-економічних завдань, підготовки та представлення аналітичних звітів.

ПР20 – Оволодіти навичками усної та письмової професійної комунікації державною та іноземною мовами.

ПР22 – Демонструвати гнучкість та адаптивність у нових ситуаціях, у роботі із новими об'єктами, та у невизначених умовах

ПР26 – Визначати необхідні комп'ютерні програми та засоби візуальної аналітики для обробки великих масивів даних з метою виявлення нових закономірностей та тенденцій.

ПР27 – Володіти навичками розробки, використання та супроводу баз даних, програмних продуктів та web-аплікацій для організації економічної діяльності в мережі Інтернет та інформатизації всіх сфер життєдіяльності суспільства.

Після завершення цього курсу студент буде :

а) знати

	<ul style="list-style-type: none"> • основні поняття та категорії інформаційної безпеки, кібербезпеки та захисту інформації; • нормативно-правову базу України у сфері захисту інформації та кібербезпеки; • види загроз інформаційній безпеці та основні канали витоку інформації; • принципи побудови систем захисту інформації в інформаційно-комунікаційних системах; • класифікацію інформації за рівнем доступу та способи її захисту; • основи криптографії, симетричні та асиметричні алгоритми шифрування; • принципи функціонування електронного цифрового підпису та електронних довірчих послуг; • методи захисту комп'ютерних мереж, VPN-технології; • види шкідливого програмного забезпечення та способи його нейтралізації; • сучасні тенденції розвитку технологій захисту інформації. <p>б) уміти</p> <ul style="list-style-type: none"> • ідентифікувати та аналізувати загрози інформаційній безпеці в організації; • оцінювати ризики витоку або втрати інформації; • розробляти базові заходи та рекомендації щодо підвищення рівня інформаційної безпеки; • застосовувати криптографічні методи для захисту даних (на концептуальному рівні); • будувати схеми захищеної передачі даних у мережі; • розробляти правила безпечної роботи з інформаційними ресурсами; • аналізувати інциденти інформаційної безпеки та пропонувати заходи реагування; • використовувати нормативні документи при розробці політик безпеки; • працювати з сучасними інформаційними ресурсами та стандартами у сфері кібербезпеки.
Ключові слова	Конфіденційна інформація, електронний ключ, е-токен, криптографія, симетричне шифрування, асиметричне шифрування, електронний цифровий підпис, еліптичне шифрування, управління ключами, хешування, аутентифікація, безпека мережі, електронний сертифікат, комп'ютерні злочини, комп'ютерні віруси.
Формат курсу	Очний
Теми	Див. Схему курсу
Підсумковий контроль, форма	Екзамен.
Пререквізити	Для опанування курсу здобувачі вищої освіти мають володіти базовими знаннями з таких освітніх компонентів, як «Інформаційні та комунікаційні технології», «Технології Інтернет», «Інформаційні системи в управлінні», «Комп'ютерні мережі», «Технологія проектування і адміністрування БД і СД» та ін.
Навчальні методи та техніки, які	У межах дисципліни застосовується поєднання традиційних, інтерактивних і практично-орієнтованих методів навчання, спрямованих на формування аналітичних, технічних і професійних компетентностей здобувачів:

<p>будуть використовуватися під час викладання курсу</p>	<p>– <i>Лекційні заняття</i> (лекції з мультимедійними презентаціями; лекції-бесіди; лекції-візуалізації з використанням схем криптографічних алгоритмів, моделей загроз, структур систем захисту інформації; аналіз практичних кейсів кіберінцидентів; застосування методів аналізу та оцінювання ризиків інформаційної безпеки);</p> <p>– <i>Лабораторні роботи</i> (виконання індивідуальних завдань у сфері захисту інформації; аналіз типових та змодельованих ситуацій інформаційної безпеки; дослідження принципів функціонування криптографічних і мережових механізмів захисту; формування навичок застосування сучасних засобів і методів забезпечення конфіденційності, цілісності та доступності інформації);</p> <p>– <i>Інтерактивні та цифрові методи</i> (використання онлайн-платформ і спеціалізованих цифрових інструментів для моделювання процесів захисту інформації, аналізу вразливостей, візуалізації результатів досліджень і представлення аналітичних висновків; застосування елементів кейс-методу та ситуаційного аналізу у сфері інформаційної безпеки);</p> <p>– <i>Самостійна робота</i> (поглиблене опрацювання теоретичних і прикладних аспектів захисту інформації; виконання індивідуальних завдань із аналізу загроз та оцінювання ризиків інформаційної безпеки; підготовка аналітичних матеріалів щодо сучасних кіберзагроз і механізмів протидії; опрацювання наукових джерел і нормативно-правових документів; рефлексія та робота над помилками).</p> <p>Застосування такого підходу забезпечує не лише ґрунтовне засвоєння теоретичних засад інформаційної безпеки, а й розвиток практичних навичок виявлення загроз, аналізу ризиків, обґрунтування заходів захисту та оцінювання їх ефективності в сучасних інформаційних системах.</p>
<p>Необхідне обладнання</p>	<p>Комп'ютерне та мультимедійне обладнання; програмне забезпечення загального призначення; засоби комунікації та управління освітнім процесом (Microsoft Teams, Moodle, Microsoft Forms, Microsoft Outlook); спеціалізовані або безкоштовні інструменти для моделювання та аналізу інформаційної безпеки, криптографії та мережевого захисту; сервіси для візуалізації результатів досліджень та організації проектної роботи.</p>
<p>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</p>	<p>Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:</p> <ul style="list-style-type: none"> • лабораторні роботи: 40% семестрової оцінки; максимальна кількість балів – 40; • самостійна робота: 10% семестрової оцінки; максимальна кількість балів – 10; • екзамен: 50% семестрової оцінки; максимальна кількість балів – 50. <p>Підсумкова максимальна кількість балів – 100.</p> <p>Політика щодо дедлайнів та перескладання: Здобувачі зобов'язані дотримуватись термінів визначених для виконання усіх видів робіт, передбачених ОК.</p> <p>Академічна доброчесність: Дотримання академічної доброчесності є обов'язковою вимогою освітнього процесу та передбачає самостійне виконання здобувачами вищої освіти всіх видів навчальних завдань, обов'язкове посилання на використані джерела та надання достовірної інформації про результати власної роботи відповідно до Положення про академічну доброчесність ЛНУ імені Івана Франка (http://www.lnu.edu.ua/wpcontent/uploads/2019/06/reg_academic_virtue.pdf). Виявлення ознак академічної недоброчесності в роботах здобувача вищої освіти є підставою для їх незарахування викладачем незалежно від</p>

масштабів запозичень або обману.

Відвідання занять: всі здобувачі мають відвідувати лекційні/лабораторні заняття.

Література: здобувачі заохочуються до використання додаткових джерел літератури, яких немає у рекомендованих.

Політика виставлення балів: враховуються бали, набрані зі всіх видів передбачених робіт. При цьому обов'язковою є присутність на заняттях та активність здобувача під час занять; недопустимість пропусків; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття, якщо це пов'язано з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін.

Жодні форми порушення академічної доброчесності не толеруються.

Критерії оцінювання знань за видами робіт

№ з/п	Види робіт. Критерії оцінювання знань студентів	Бали рейтингу	Максимальна кількість балів
1	2	3	4
1. Бали поточної успішності за виконання лабораторних робіт			
Критерії оцінювання		5 балів	
Завдання виконано повністю, правильно та самостійно; результати коректні, висновки обґрунтовані; студент впевнено пояснює виконані дії.		5	
Завдання виконано переважно правильно; наявні окремі неточності або неповні висновки; студент загалом орієнтується в матеріалі.		3-4	
Завдання виконано частково; допущено суттєві помилки; пояснення неповні або поверхневі.		1-2	
Завдання не виконане або формально; результати відсутні; студент не може пояснити дії		0	
2. Самостійна робота студентів (СРС)			
Критерії оцінювання		10 балів	
Проект: «Аналіз загроз та базове шифрування»			
Повнота та коректність виконання завдання (макс. 4 бали)		4	
– 4 бали – завдання виконано повністю; коректно визначені загрози, описано механізм їх реалізації; правильно реалізовано базове шифрування; результати відповідають вимогам.			
– 3 бали – завдання виконано в основному правильно; наявні незначні неточності в описі загроз або реалізації шифрування.			
– 2 бали – завдання виконано частково; пропущено окремі етапи або допущено суттєві помилки.			
– 1 бал – робота має фрагментарний характер; більшість вимог не виконано.			
– 0 балів – завдання не виконано або не відповідає темі.			

	<p>Обґрунтованість рішень та аналіз результатів (макс. 3 бали)</p> <ul style="list-style-type: none"> – 3 бали – результати логічно проаналізовані; студент аргументовано пояснює вибір методів і отримані висновки. – 2 бали – аналіз загалом правильний, але неповний або недостатньо глибокий. – 1 бал – пояснення поверхневі; аргументація слабка. – 0 балів – аналіз відсутній. 	3
	<p>Оформлення та креативність (макс. 3 бали)</p> <ul style="list-style-type: none"> – 3 бали – робота виконана самостійно; матеріал структурований; оформлення відповідає вимогам. – 2 бали – загалом вимоги дотримано, але є незначні недоліки в структурі або поданні матеріалу. – 1 бал – оформлення неповне або неструктуроване; є ознаки формального підходу. – 0 балів – відсутня самостійність або робота не оформлена належним чином. 	3
3. Екзамен		
Критерії оцінювання		50 балів
Встановлено 3 рівні складності завдань		
	<p>1. Перший рівень (завдання 1) – завдання із вибором відповіді – тестові завдання. Завдання з вибором відповіді на теоретичне питання вважається виконаним правильно, якщо в картці тестування записана правильна відповідь.</p>	10*2=20
	<p>2. Другий рівень (завдання 2) – завдання з короткою відпо- віддю. Завдання з короткою відповіддю вважається виконаним правильно, якщо студент дав вірні визначення, посилання, тлу- мачення, короткі коментарі.</p>	2*5=10
	<p>3. Третій рівень (завдання 3) – практичне завдання. Практичне завдання вважається виконаним правильно, якщо воно виконано у повному обсязі, без помилок.</p>	20

Таблиця оцінювання (визначення рейтингу)
навчальної діяльності студентів

Поточний контроль		Екзамен – 50 балів	РАЗОМ – 100 балів
Лабораторні заняття	СР		
40	10		

Шкала оцінювання успішності студентів за результатами
підсумкового контролю

Оцінка ECTS	Оцінка в балах	Оцінка за національною шкалою	
		Екзамен, диференційований залік	Залік
A	90-100	5	Відмінно
B	81-89	4	Дуже добре
C	71-80		Добре
D	61-70	3	Задовільно
E	51-60		Достатньо

	<p>48. Вразливість VPN. 49. Резервне копіювання. 50. Адміністрування інформаційних систем. 51. Безпека протоколів TCP/IP. 52. Трендові напрями в сфері інформаційної безпеки. 53. Програмні засоби захисту інформації. 54. Інформаційні технології та право. 55. Комп'ютерні злочини. 56. Правила роботи з WWW. 57. Обов'язки користувача. 58. Правила використання електронної пошти. 59. Адміністрування електронної пошти. 60. Використання електронної пошти для конфіденційного обміну інформацією. 61. Комп'ютерні віруси та їх властивості. 62. Класифікація вірусів. 63. Основні види комп'ютерних вірусів та схеми їх функціонування. 64. Структура комп'ютерних вірусів. 65. Програми виявлення вірусів та заходи по захисту та профілактиці. 66. Антивірусні пакети.</p>
<p>Неформальна та інформальна освіта</p>	<p>Здобувачі мають право на визнання (перезарахування) результатів навчання, набутих у неформальній та інформальній освіті відповідно до «Порядку визнання у Львівському національному університеті імені Івана Франка результатів навчання, здобутих у неформальній та інформальній освіті (нова редакція)» https://education-quality.lnu.edu.ua/wp-content/uploads/2024/05/Nova-redaktsiia-polozhennia-pro-neformalnu-ta-informalnu-osvitu.pdf Шляхи здобуття знань у неформальній освіті: онлайн-курси на платформах Prometheus, Coursera, EdEra, Genesis та ін.; різноманітні тренінги, семінари й вебінари, літні / зимові школи тощо. При цьому, знання та навички, що формуються під час їх проходження, повинні мати зв'язок з очікуваними навчальними результатами даної дисципліни. Можливе перезарахування: тем/теми змістових модулів, які співвідносні за змістовим наповненням до знань, отриманих шляхом неформальної освіти; якщо отримані в неформальній освіті знання поглиблюють і розширюють тему / теми змістових модулів; тем / теми лабораторних занять, які співвідносні за змістовим наповненням до знань, отриманих шляхом неформальної освіти; якщо отримані в неформальній освіті знання поглиблюють і розширюють тему / теми лабораторних занять; тем / теми самостійної роботи, які співвідносні за змістовим наповненням до знань, отриманих шляхом неформальної освіти; якщо отримані в неформальній освіті знання поглиблюють і розширюють тему / теми самостійної роботи. Для визнання й перезарахування знань, отриманих у неформальній освіті, студенту слід представити сертифікат, що підтверджує здобуття знань у неформальній освіті.</p>
<p>Опитування</p>	<p>Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.</p>

Схема курсу

Тиждень / дата / год.	Тема, план, короткі тези	Форма діяльності (заняття)	Література. Ресурси в інтернеті	Завдання
1	2	3	4	5
За розкладом	ТЕМА 1. Загальні аспекти захисту інформації Загальні поняття захисту інформації. Закони України про захист інформації. Види інформації за правом доступу. Поняття інформаційної безпеки. Концепції та моделі інформаційної безпеки. Види загроз інформаційній безпеці та їх характеристики. Канали витоку інформації.	Лекція 2 год.	Осн.: [2, 4-9, 11] Дод.: [1-4, 5] Інт.: [1, 3, 4]	Опрацювати лекційний матеріал, виконати завдання для самоконтролю та підготуватися до лабораторного заняття
За розкладом	ТЕМА 1. Загальні аспекти захисту інформації Операції, що використовуються у криптографії.	Лабораторна робота 2 год.	Осн.: [2, 4-9, 11] Дод.: [1-4, 5] Інт.: [1, 3, 4]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 1. Загальні аспекти захисту інформації Операції, що використовуються у криптографії.	Лабораторна робота 2 год.	Осн.: [2, 4-9, 11] Дод.: [1-4, 5] Інт.: [1, 3, 4]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 1. Загальні аспекти захисту інформації Важливість і складність проблеми інформаційної безпеки. Політика інформаційної безпеки. Кібербезпека як чинник національної безпеки України.	Лекція 2 год.	Осн.: [2, 4-9, 11] Дод.: [1-4, 5] Інт.: [1, 3, 4]	Опрацювати лекційний матеріал, виконати завдання для самоконтролю та підготуватися до лабораторного заняття

1	2	3	4	5
За розкладом	ТЕМА 1. Загальні аспекти захисту інформації Робота з функціями, що використовуються в теорії чисел та криптографії.	Лабораторна робота 2 год.	Осн. [1-5, 7, 9-11]. Дод. [1, 6]. Інт. [2-5].	Обговорити проблемні питання, виконати завдання.
За розкладом	ТЕМА 1. Загальні аспекти захисту інформації Робота з функціями, що використовуються в теорії чисел та криптографії. Самостійна робота (підзавдання до теми 1) Проект: «Аналіз загроз та базове шифрування» Проаналізувати основні загрози інформаційній безпеці обраної організації, дослідити їхні характеристики, ймовірність виникнення та вплив на бізнес-процеси; сформулювати рекомендації щодо базових заходів захисту.	Лабораторна робота 2 год., СРС 18 год.	Осн. [1-5, 7, 9-11]. Дод. [1, 6]. Інт. [2-5].	Обговорити проблемні питання, виконати завдання.
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Засоби захисту інформації від несанкціонованого доступу. Міжнародні правила застосування шифру. Управління криптографією. Вимоги до криптографічних систем.	Лекція 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Опрацювати лекційний матеріал, виконати завдання для самоконтролю та підготуватися до лабораторного заняття
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Знайомство з простими методами шифрування.	Лабораторна робота 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Знайомство з простими методами шифрування.	Лабораторна робота 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Обговорити проблемні питання, виконати завдання

1	2	3	4	5
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Класифікація криптографічних методів.	Лекція 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Опрацювати лекційний матеріал, виконати завдання для самоконтролю та підготуватися до лабораторного заняття
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Знайомство з простими методами шифрування.	Лабораторна робота 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Знайомство з простими методами шифрування.	Лабораторна робота 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Проблеми та перспективи криптографічних систем. Управління ключами. Розподіл ключів та Public Key Infrastruture.	Лекція 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Опрацювати лекційний матеріал, виконати завдання для самоконтролю та підготуватися до лабораторного заняття
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Алгоритм Евкліда.	Лабораторна робота 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Обговорити проблемні питання, виконати завдання

1	2	3	4	5
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Алгоритм Евкліда.	Лабораторна робота 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Правове, організаційне та технічне забезпечення режиму електронного цифрового підпису.	Лекція 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Опрацювати лекційний матеріал, виконати завдання для самоконтролю та підготуватися до лабораторного заняття
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Розширений метод Евкліда.	Лабораторна робота 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 2. Криптографічні методи захисту інформації Розширений метод Евкліда.	Лабораторна робота 2 год.	Осн.: [2-4, 10] Дод.: [5, 6-8] Інт.: [1, 2]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 3. Безпека в інформаційних мережах Фізична безпека. Механізми захисту в операційній системі. Загальна характеристика систем захисту в інформаційних мережах. Ідентифікація та автентифікація. Користувацький інтерфейс. Телекомунікації та віддалений доступ. Технології VPN. Поняття протоколу, комунікаційний та криптографічний протоколи. Основи побудови VPN. Вразливість VPN. Резервне копіювання даних. Адміністрування інформаційних систем. Трендові напрями в сфері інформаційної безпеки.	Лекція 2 год.	Осн.: [2, 4-7, 8-9] Дод.: [5] Інт.: [1, 3, 4]	Опрацювати лекційний матеріал, виконати завдання для самоконтролю та підготуватися до лабораторного заняття

1	2	3	4	5
За розкладом	ТЕМА 3. Безпека в інформаційних мережах Симетричні методи шифрування повідомлень.	Лабораторна робота 2 год.	Осн.: [2, 4-7, 8-9] Дод.: [5] Інт.: [1, 3, 4]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 3. Безпека в інформаційних мережах Симетричні методи шифрування повідомлень.	Лабораторна робота 2 год.	Осн.: [2, 4-7, 8-9] Дод.: [5] Інт.: [1, 3, 4]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 4. Правила безпеки в Internet Інформаційні технології та право. Комп'ютерні злочини. Правила роботи з . Обов'язки користувача. Правила використання електронної WWW пошти. Адміністрування електронної пошти. Використання електронної пошти для конфіденційного обміну інформацією.	Лекція 2 год.	Осн.: [2, 4-7] Дод.: [4] Інт.: [1, 3]	Опрацювати лекційний матеріал, виконати завдання для самоконтролю та підготуватися до лабораторного заняття
За розкладом	ТЕМА 3. Безпека в інформаційних мережах Методи шифрування та дешифрування інформації.	Лабораторна робота 2 год.	Осн.: [2, 4-7, 8-9] Дод.: [5] Інт.: [1, 3, 4]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 3. Безпека в інформаційних мережах Методи шифрування та дешифрування інформації.	Лабораторна робота 2 год.	Осн.: [2, 4-7, 8-9] Дод.: [5] Інт.: [1, 3, 4]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 5. Програмні віруси та способи їх нейтралізації Комп'ютерні віруси та їх властивості. Класифікація вірусів. Основні види комп'ютерних вірусів та схеми їх функціонування. Структура комп'ютерних вірусів. Програми виявлення вірусів та заходи по захисту та профілактиці. Антивірусні пакети.	Лекція 2 год.	Осн.: [2, 4-9] Дод.: [5] Інт.: [1, 3, 4]	Опрацювати лекційний матеріал, виконати завдання підготуватися до лабораторного заняття

1	2	3	4	5
За розкладом	ТЕМА 3. Безпека в інформаційних мережах Методи шифрування та дешифрування інформації.	Лабораторна робота 2 год.	Осн.: [2, 4-7, 8-9] Дод.: [5] Інт.: [1, 3, 4]	Обговорити проблемні питання, виконати завдання
За розкладом	ТЕМА 3. Безпека в інформаційних мережах Методи шифрування та дешифрування інформації. Самостійна робота (підзавдання до теми 3) Проект: «Аналіз загроз та базове шифрування» Провести моделювання базового шифрування повідомлення (AES у режимі CBC); проаналізувати отримані результати, пояснити застосовані методи та оцінити ефективність обраного способу захисту інформації.	Лабораторна робота 2 год., СРС 18 год.	Осн.: [2, 4-7, 8-9] Дод.: [5] Інт.: [1, 3, 4]	Обговорити проблемні питання, виконати завдання

Викладач  Анна ЗАДОРОЖНА