МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ІВАНА ФРАНКА

Кафедра безпеки інформації та бізнес-комунікацій

Затверджено
на засіданні кафедри безпеки інформації та бізнес-комунікацій
економічного факультету
Львівського національного університету імені Івана Франка
(протокол №1 від 30.08.2022 р.)

В.о. зав. кафедри проф. М.І. Хмелярчук

СИЛАБУС З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ІНФОРМАЦІЙНА БЕЗПЕКА»,

що викладається в межах ОПП

«Економічна кібернетика та бізнес-аналітика»

першого (бакалаврського) рівня вищої освіти для здобувачів зі спеціальностей : 051 «Економіка»

Львів - 2022 р.

Назва курсу	“ Інформаційна безпека ”
Адреса викладання дисципліни	м. Львів, проспект В'ячеслава Чорновола, 61, аудиторія ___
Факультет та кафедра, за якою закріплена дисципліна	Економічний факультет, кафедра безпеки інформації та бізнес-комунікацій
Галузь знань, шифр та назва спеціальності	05 Соціальні та поведінкові науки 051 Економіка
Ступінь вищої освіти	Бакалавр
Статус дисципліни	вибіркова навчальна дисципліна
Семестр	7
Форма навчання	Денна
Обсяг дисципліни, кредити ЄКТС / загальна кількість годин	6 кредитів / 180 годин
Викладач (-і)	Циганчук Роман Олегович, кандидат економічних наук, доцент, доцент кафедри безпеки інформації та бізнес-комунікацій економічного факультету
Контактна інформація викладача (-ів)	Профайл викладача курсу: https://econom.lnu.edu.ua/employee/tsyhanchuk-roman-olehovych Електронна пошта roman.tsyhanchuk@lnu.edu.ua
Консультації з питань вивчення дисципліни	У день проведення практичних занять, 16.00-17.00 год. (м. Львів, проспект В'ячеслава Чорновола, 61, аудиторія ___)
Мова викладання	Українська
Сторінка курсу	

ІНФОРМАЦІЯ ПРО ДИСЦИПЛІНУ

Коротка анотація дисципліни	Силабус вибіркової навчальної дисципліни «Інформаційна безпека» складений відповідно до освітньо-професійної програми підготовки фахівця освітнього ступеня «бакалавр». Вивчення дисципліни «Інформаційна безпека» спрямоване на формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів захисту інформації у сучасних інформаційних системах та мережах і лініях телекомунікаційного зв’язку в умовах широкого використання сучасних інформаційних технологій.
Мета дисципліни	**Мета** вивчення дисципліни: формування термінологічного фундаменту; навчання студентів правильно проводити аналіз загроз інформаційній безпеці; ознайомити з основними методами, принципами, алгоритмами захисту інформації в комп’ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

	Завданням дисципліни є ознайомлення студентів з основними методами обробки інформації, існуючими технологіями захисту інформації і практичними навичками з їх створення, впровадження і супроводження.
Література для вивчення дисципліни	**Базова:** 1. Закон України «Про електронний цифровий підпис»; 2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»; 3. Закон України «Про інформацію»; 4. Закон України "Про захист інформації в автоматизованих системах" 5. Вимоги до системи управління інформаційною безпекою. СОУ Н НБУ 65.1 СУІБ 1.0:2010, СОУ Н НБУ 65.1 СУІБ 2.0:2010. 6. Положення про контроль за функціонуванням системи технічного захисту інформації. Затверджено наказом ДСТСЗІ СБ України від 22.12.99.№ 61. 7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423. 8. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53. 9. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22. 10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22. 11. В. Фурашев. Питання законодавчого визначення понятійно-категоріального апарату у сфері інформаційної безпеки // “Інформація і право”. – № 1(4)/2012. – С. 46 – 55. 12. В. Фурашев Сутність та визначення понять “інформаційна безпека” і “безпека інформації” // “Правова інформатика”. – № 2(34)/2012. – С. 51 – 59. 13. Фурашев В.М. Ключові аспекти проекту Закону України “Про безпеку інформації” // “Віче”. – 2012. – № 6/2012(315). – С. 29 – 30. 14. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 30 с. 15. National Military Strategy for Cyberspace Operations. – Режим доступу : //www.dod. gov/pubs/foi/ojcs/07-F-2105doc1.pdf 16. Glossary and Acronyms (Archived) / European Commission. – (Accessed 03 Nov 2009). – Режим доступу : //www.ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c 17. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space. – Режим доступу : //www.official-document/cm76/7642/7642.pdf 18. The French White Paper on defence and national security. – Режим доступу : //www.livreblancdefenseetsecurite.gouv.fr/IMG/pdf/white_paper_press_kit.pdf 19. Новицький Г.В. Теоретико-правові основи забезпечення національної безпеки України / Г.В. Новицький. – К. : Інтертехнологія, 2008. – 496 с. 20. Хлевицький В.Б. Інформаційна безпека як одна із складових національної безпеки України / В.Б. Хлевицький // Євроатлантикінформ. – 2006. – № 1(7). – С. 70 – 72. 21. Бачило И.Л. Методология решения правовых проблем в области информационной безопасности / І.Л. Бачило // Информатика и вычислительная техника. – 1992. – №2. – С. 22 – 30. 22. Брижко В. До питання застосування у правотворчості понять “інформація” та “дані” / В. Брижко // Правова інформатика. – 2005. – № 4 (8). – С. 31 – 37. 23. Калюжний Р. Проблеми та перспективи правового забезпечення безпеки

	інформації з обмеженим доступом, що не становить державної таємниці / Р. Калюжний, Д. Прокоф'єва // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник / НТУУ "КПІ", Міністерство освіти і науки України, Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України. – К., 2000. – С. 27 – 31. 24. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : монографія / Б.А. Кормич. – Одеса : Юридична література, 2003. – 472 с. 25. Марущак А.І. Правомірні засоби доступу громадян до інформації : науково-практичний посібник / А.І. Марущак. – Біла Церква : Вид-во "Буква", 2006. – 432 с. 26. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : монографія / В.Б. Толубко. – К. : НАОУ, 2003. – 315 с. 27. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України : аналітична доповідь / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 30 с. 28. Колодюк О.В. Національні стратегії інформаційного суспільства: необхідність, переваги та стан щодо запровадження в Україні / О.В. Колодюк – Режим доступу : http: //www.isu.org.ua/viewarticale/publications/117?new_lang=u.
Обсяг курсу	64 годин аудиторних занять, з них 32 години лекцій, 32 годин практичних занять та 116 годин самостійної роботи
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент повинен **знати:** – теорію побудови систем захисту інформації; – криптографічні методи обробки інформації; – технології зберігання інформації; – методи захисту від комп'ютерних вірусів; – основи технології контролю мережевого трафіку. **вміти:** – виконувати розрахунки контрольних сум, надмірних циклічних кодів; – проводити перетворення інформації з метою передачі за каналами зв'язку; – аналізувати захищеність комп'ютерних мереж від зовнішніх загроз, користуватися спеціальною та довідковою літературою; – розробляти захищені вузли з обробки інформації.
Ключові слова	Безпека, інформаційна система, загроза, несанкціонований доступ, захист інформації, інцидент, канал витоку інформації, криптографія, стеганографія.
Формат курсу	Денний Проведення лекцій, практичних занять, консультацій
Теми	Тема 1. Основи безпеки інформаційних систем. Тема 2. Канали витоку інформації. Тема 3. Захист інформації від ненавмисних загроз. Тема 4. Захист від несанкціонованого доступу. Тема 5. Технічні методи та засоби захисту інформації в інформаційних системах. Тема 6. Теорія оптимальних систем. Тема 7. Програмні методи та засоби захисту інформації. Тема 8. Захист інформації в розподілених інформаційних системах. Тема 9. Система управління інцидентами інформаційної безпеки. Тема 10. Організаційно-правове забезпечення захисту інформації.
Підсумковий	***Критерії оцінювання***

контроль, форма	1. Критерієм успішного проходження здобувачем освіти оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни. 2. Мінімальний пороговий рівень оцінки варто визначати за допомогою якісних критеріїв і трансформувати його в мінімальну позитивну оцінку числової (рейтингової) шкали, що використовується. ***Засоби оцінювання*** Засобами оцінювання результатів навчання можуть бути: – стандартизовані тести; – аналітичні звіти, реферати, есе; – розрахункові та розрахунково-графічні роботи; презентації результатів виконаних завдань та досліджень; розрахункові роботи; – інші види індивідуальних та групових завдань. ***Форми поточного та підсумкового контролю*** 1. Форма підсумкового контролю за навчальною дисципліною «Інформаційна безпека» - залік. 2. Форми поточного контролю під час навчальних занять: усні відповіді. Розв'язування задач та практичних завдань, письмове опитування у формі самостійних та контрольних робіт, написання економічних есе.
Пререквізити	Вивчення дисципліни «Інформаційна безпека» спрямоване на формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів захисту інформації у сучасних інформаційних системах та мережах і лініях телекомунікаційного зв'язку в умовах широкого використання сучасних інформаційних технологій. Міждисциплінарні зв`язки: дисципліна «Інформаційна безпека» ґрунтується на знаннях, отриманих при вивченні таких курсів як «Економічний аналіз», «Цифрова економіка», «Вища математика», «Теорія ймовірностей», «Інформаційні технології (рівень А)» та інших курсів.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Інтерактивні лекції (проблемні лекції, лекції-дискусії, лекції-демонстрації з використанням мультимедійного обладнання); Практичні заняття (навчальні дискусії, мозковий штурм, розв'язок ситуаційних вправ (кейсів)); Самостійне навчання (індивідуальна робота, робота в групах). Лекції надають здобувачам основний теоретичний матеріал, що є основою для самостійного навчання, а також сприяють розвитку у здобувачів вищої освіти здатності до узагальнення та критичного мислення через участь в дискусіях. Лекції доповнюються практичними заняттями, що надають здобувачам вищої освіти можливість застосовувати теоретичні знання на реальних прикладах. Практичні заняття сконструйовані з застосуванням методів практико-орієнтованого навчання, і передбачають розв'язок здобувачами вищої освіти кейсів на основі можливих реальних ситуацій та виконання

<table>
<tr><td></td><td>необхідних розрахунків. Самостійне навчання сприяє підготовці до лекцій, практичних занять, а також роботи індивідуально та в невеликих групах для підготовки презентацій, що будуть представлені іншим групам, та для виконання індивідуальних та групових ситуаційних вправ на практичних заняттях, участі в них тощо.</td></tr>
<tr><td>Необхідні обладнання</td><td>Мультимедіа та проекційна апаратура.
Комп'ютери, комп’ютерні системи та мережі.
Бібліотечні фонди.</td></tr>
<tr><td>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</td><td>
<table>
<tr><td rowspan="2">Форми контролю</td><td>Максимальна кількість балів</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Поточний контроль:</td><td></td></tr>
<tr><td>Усні відповіді, розв’язування задач та практичних завдань</td><td>10 х 5 = 50 балів</td></tr>
<tr><td>Письмові опитування</td><td>до 30 балів</td></tr>
<tr><td>Підсумкова контрольна робота</td><td>20 балів</td></tr>
<tr><td>Всього за результатами поточного контролю:</td><td>100</td></tr>
<tr><td>Всього</td><td>100</td></tr>
</table>
Письмові роботи: Очікується, що студенти виконають декілька видів письмових робіт (есе, вирішення кейсу).
Академічна доброчесність: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману.
Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції і практичні зайняття курсу. Студенти мають інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов’язані дотримуватися усіх строків визначених для виконання усіх видів письмових робіт, передбачених курсом.
Жодні форми порушення академічної доброчесності <u>не толеруються</u>.</td></tr>
<tr><td>Контрольні запитання</td><td>1. Що являє собою поняття інформаційної сфери?
2. Що є інформаційними ресурсами країни?
3. Як можна визначити поняття інформаційної війни та інформаційної зброї?
4. Які складові включає у себе інформаційна інфраструктура?
5. Надайте визначення інформаційної безпеки.
6. Які базові засади інформаційної безпеки нашої держави закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України?
7. Які правові основи інформаційної діяльності закладено у Закон України “Про інформацію”?
8. Як поділяється інформація за режимом доступу до неї?
9. Як здійснюється контроль за режимом доступу до інформації?
10. Яка інформація відноситься до таємної інформації?
11. Які грифи таємності можуть надаватися інформації та який їх терміни дії?
12. Які національні інтереси України потрібно захищати у відповідності до Закону України “Про основи національної безпеки України” та “Концепції національної безпеки України”?
13. Що визначає “Концепція національної безпеки України”?
14. Що визначає та має забезпечити “Концепція технічного захисту інформації в Україні”?</td></tr>
</table>

	15. Що складає правову основу забезпечення ТЗІ в Україні? 16. Які принципи формування і проведення державної політики у сфері ТЗІ? 17. Які основні функції організаційних структур системи ТЗІ? 18. Які глобальні проблеми інформаційної безпеки виникають у світі у зв'язку з сучасним станом розвитку інформаційних технологій та, зокрема, мережі Інтернет? 19. Чим відрізняються сучасні методи Інтернет-атак? 20. Які особливості сучасних хакерських програм та практики їх застосування? 21. Які різновиди вірусів Вам відомі? 22. Надайте класифікацію комп'ютерних вірусів за методами проникнення та маскування у системі. 23. Надайте класифікацію комп'ютерних вірусів за методами похищення інформації. 24. Які сучасні методи та програми антивірусного захисту Вам відомі? 25. Надайте класифікацію методів та програм антивірусного захисту. 26. На яких складових ІС може здійснюватися захист від НСД? 27. Які системи використовуються для захисту інформації на рівні прикладного й системного ПЗ? 28. Які засоби мережевого захисту інформації використовуються у комунікаційних системах? 29. Надайте визначення програмних засобів захисту інформації. 30. Які мають риси та які функції забезпечують засоби криптографічного захисту інформації? 31. Які основні функції реалізують програмні засоби захисту? 32. Чим гарантується визначений рівень захищеності засобів захисту інформації? 33. Надайте визначення блокування інформації в системі. 34. Надайте визначення витоку інформації в системі. 35. Надайте визначення знищення інформації в системі. 36. Надайте визначення порушення цілісності інформації в системі. 37. Що є об'єктами захисту в системі? 38. Чим може гарантуватися надійний захист інформації у системі? 39. На яких складових ІС може здійснюватися захист від НСД? 40. Що використовується для я захисту інформації на рівні апаратного забезпечення? 41. Надайте визначення програмно-апаратних засобів захисту інформації. 42. Чим гарантується визначений рівень захищеності засобів захисту інформації? 43. Надайте визначення цифрового підпису. 44. Надайте визначення віртуальних логічних дисків. 45. Які функції та параметри забезпечують утілити очищення дисків та знищення інформації? 46. Надайте визначення захисту інформації в системі. 47. Надайте визначення технічного захисту інформації в системі. 48. Надайте визначення витоку інформації в системі. 49. Що є об'єктами захисту в системі? 50. Чим може гарантуватися надійний захист інформації у системі? 51. На які класи завдань розбиваються питання ТЗІ в системах? **52. Чим забезпечується захист інформації від її витоку технічними каналами зв'язку?** 53. Чим гарантується визначений рівень захищеності засобів захисту інформації? 54. Надайте класичне визначення криптографії. 55. Надайте визначення операції шифрування. 56. Надайте визначення операції дешифрування. 57. Що є відкрита абетка? 58. Що є таємна абетка? 59. В чому полягає сенс шифру заміни? 60. В чому полягає шифр Цезара? 61. Надайте визначення криптоаналітики. 62. Надайте визначення таблиці частотності. 63. Як використовується таблиця частотності для злому шифрів заміни? 64. В чому полягає сенс шифру перестановки? 65. Що уявляє собою скитала? 66. Надайте загальне визначення алгоритму шифрування. 67. Надайте загальне визначення криптографічного ключа. 68. В чому полягає основний принцип криптографії? 69. Від чого залежить стійкість шифру? 70. Надайте загальне визначення кодування. 71. В чому полягає сенс використання номенклаторів? 72. В чому полягають основні вади кодів?

	73. В чому полягає слабкість одноабеткових шифрів заміни? 74. Яким типом шифру є шифр Віженера? 75. Яким типом шифру є омофоничний шифр? Який тип шифру покладено у основу електромеханічних шифрувальних машин? 76. Скільки шифрувальних коліс було у шифромашині “Енігма”? 77. Який принцип шифрування закладено у електромеханічних шифрувальних машинах? 78. В чому полягає принцип шифрування з використанням разового шифроблокноту? 79. Який алгоритм шифрування з використанням разового шифроблокноту? 80. В чому полягає сенс поняття відсутності критерію відкритого тексту? 81. Намалюйте модель секретного зв’язку К. Шеннона. 82. В чому полягає принцип симетричного шифрування? 83. Яким чином представлено літери у ЕОМ? 84. В чому полягає проблема розподілу ключів? 85. Які основні методи використовуються при шифруванні у ЕОМ при представленні літер у двійковому коді? 86. Дайте визначення шифрування з асиметричним ключем. 87. Як була доведена теорема існування для алгоритму шифрування з відкритим ключем? 88. Поясніть, що таке оборотна функція? 89. На прикладі складання за модулем поясніть, що таке необоротна функція. 90. Яка головна теорема модульної арифметики? 91. Як проводяться операції з числами, записаними за одним модулем? 92. Чому дорівнює лишок, отриманий у результаті цілого ділення числа на його модуль? 93. За яким правилами обираються числа p, q, e та N закритого та відкритого ключа в алгоритмі шифрування RSA? 94. Які числа публікує отримувач повідомлень як відкритий ключ? 95. За якою формулою обчислює відправник літери відкритого повідомлення для їх зашифрування в алгоритмі шифрування RSA? 96. Яке число має розрахувати отримувач для розшифрування отриманого повідомлення, зашифрованого в алгоритмі шифрування RSA? 97. За якою формулою обчислює отримувач літери закритого повідомлення для їх розшифрування в алгоритмі шифрування RSA? 98. Що складає сутність стеганографії? 99. Наведіть класифікацію стеганографічних методів. 100. Які існують методи інформаційної стеганографії? 101. Які умови повинні виконуватися при застосуванні стеганографічних методів?
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.