МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Фізичний факультет
Кафедра фізики твердого тіла

Затверджено
На засіданні кафедри фізики твердого тіла
фізичного факультету
Львівського національного університету
імені Івана Франка
(протокол № 1 від 29 серпня 2024 р.)

Завідувач кафедри _____
Володимир КАПУСТЯНИК

Силабус з навчальної дисципліни вільного вибору

«Основи інформаційної та кібербезпеки»,

що викладається в межах ОПП першого (бакалаврського) рівня вищої освіти

для студентів другого курсу всіх спеціальностей

Львів 2024 р.

Назва курсу	**Основи інформаційної та кібербезпеки**
Адреса викладання курсу	вул. Кирила і Мефодія 8, 79005 Львів
Факультет та кафедра, за якою закріплена дисципліна	фізичний факультет, кафедра фізики твердого тіла
Викладачі курсу	доцент кафедри фізики твердого тіла, к.ф.-м.н Бовгира Олег Вікторович
Контактна інформація викладачів	oleh.bovhyra@lnu.edu.ua https://physics.lnu.edu.ua/employee/bovhyra-oleh-viktorovych
Консультації по курсу відбуваються	Консультації в день проведення лекцій та практичних занять (за попередньою домовленістю). Також можливі он-лайн консультації через електронну пошту.
Сторінка курсу	https://physics.lnu.edu.ua/course/osnovy-informatsiynoi-ta-kiberbezpeky
Інформація про курс	У сучасних умовах знання з кібербезпеки у тих хто навчається повинні формуватися в рамках базових курсів всіх без винятку навчальних закладів, а не тільки спеціалізованих за ІТ та кібер- напрямами. Курс спрямований на підвищення інформаційної грамотності та правової культури студентів, оволодіння ними основоположними знаннями у сфері інформаційної безпеки та основними правовими механізмами її забезпечення; набуття базових знань та умінь щодо ефективного і безпечного поводження з інформацією; підготовкою у питаннях розпізнавання об'єктів та носіїв інформаційної небезпеки, формування власного бачення щодо сутності, проявів, наслідків та механізмів інформаційної безпеки.
Коротка анотація курсу	Навчальний курс «Основи інформаційної та кібербезпеки» є дисципліною вільного вибору для першого (бакалаврського) рівня вищої освіти усіх спеціальностей Університету, яка викладається в 3 семестрі в обсязі 3 кредитів (за Європейською Кредитно-Трансферною Системою ECTS). **Зміст курсу**: • Сутність інформаційної безпеки. • Правові питання забезпечення інформаційної безпеки. • Загальні поняття про організацію захисту від їх деструктивного впливу кібератак. • Захист персональних даних та захист приватності. • Забезпечення безпеки у кіберпросторі. • Інсайдерство та соціальна інженерія.
Мета та цілі курсу	Метою і завданням навчальної дисципліни є формування знань щодо сутності інформаційної безпеки та кібербезпеки як складного багаторівневого явища, що має соціальні, психологічні й технічні виміри. Результатом вивчення дисципліни є формування та/або розвиток навичок виявлення і протидії інформаційним загрозам на рівні людини, суспільства та держави. Здобувачі вищої освіти також вивчатимуть положення нормативно-правових актів, які спрямовані на забезпечення інформаційних прав та свобод людини і громадянина та захист інтересів держави в інформаційній сфері

Література для вивчення дисципліни	**Базова:** 1. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. – 2017. – № 5. – С. 15. – Ст. 102. https://www.president.gov.ua/documents/472017-21374 2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text 3. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96/2016// Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899. https://zakon.rada.gov.ua/laws/show/96/2016#Text 4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко – К. : ДУТ - КНУ, 2016. – 178 с. 5. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015. – 288 с. 6. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 2008. – 352 с. 7. Словник термінів з кібербезпеки / За загальною редакцією Копана О.В., Скулиша Є.Д. –К. : ВБ «Аванпост-Прим». – 2012. – 214 с. 8. Інформаційна безпека держави : підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.] ; в 2 т. – Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2016. – 264 с. 9. Дудатьєв А. В.Захист комп'ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А. – Вінниця ВНТУ, 2010. – 219 с. 10. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с. **Допоміжна:** 1. Про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. № 994-575. https://zakon.rada.gov.ua/laws/show/994_575#Text 2. Про інформацію : Закон України від 02.10.92 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650. https://zakon.rada.gov.ua/laws/show/2657-12#Text 3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text Інформаційна безпека держави : підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.] ; в 2 т. – Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2016. – 264 с. 5. Законодавчі основи забезпечення інформаційної безпеки України: наукова доповідь / Пилипчук В.Г., Корж І.Ф., Петришин О.В.,

	Савінова Н.А., Фурашев В.М. (За заг. ред. Пилипчука В.Г.) – К: НДІІП НАПрН України, 2014. – 60 с. 6. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова- Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. /В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко/ –К.:ДУТ, 2015. – 345 с. 7. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с. 8. Хорошко В.О. Основи комп'ютерної стеганографії / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця.: ВДТУ, 2003. – 142 с. 9. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с. **Інформаційні ресурси:** 1. Системи онлайн-освіти: https://prometheus.org.ua/, https://www.coursera.org, http://www.udacity.com, 2. Портал безпека [Електронний ресурс]. – Режим доступу: https://www.bezpeka.com/uk/golovna/ 3. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/ 4. Державна служба спеціального зв'язку та захисту інформації: [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua 5. Команда реагування на комп'ютерні надзвичайні події України: [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/
Тривалість курсу	один семестр
Обсяг курсу	3 кредити ЄКТС, 90 годин, з яких 32 години аудиторних занять, з них 16 годин лекцій, 16 годин практичних занять, та 58 годин самостійної роботи
Очікувані результати навчання	В результаті вивчення цього курсу студент отримає *компетенції*: здатність застосовувати відповідні математичні, наукові і технічні методи, а також спеціалізоване програмне забезпечення для вирішення завдань в сфері інформаційної та кібербезпеки; здатність використовувати практичні навички в сфері інформаційної та кібербезпеки, здатність продемонструвати розуміння проблем інформаційної та кібербезпеки. Вміння: оцінювати поточний стан рівня інформаційної та кібербезпеки; аргументувати вибір та застосовування методів і засобів для побудови захищених інформаційних систем у кіберпросторі; використовувати сучасну нормативну базу у галузі інформаційної та кібербезпеки; виконувати аналіз загроз та вразливостей критичних систем; використовувати методи та засоби виявлення та аналізу вразливостей та атак на кіберпростір; використовувати ресурси, на яких публікуються виявлені вразливості та атаки.
Формат курсу	Очний
	проведення лекцій, лабораторних робіт та консультації для кращого розуміння тем

Теми	Наведено у табл.1 і табл. 2
Підсумковий контроль, форма	залік в кінці семестру комбінований
Пререквізити	Для вивчення курсу необхідні знання з таких предметів: “Вища математика”, “Програмування і математичне моделювання”.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Використовуються такі методи навчання: а) *словесні* – лекція, пояснення, бесіда, інструктаж (вступний та поточний) під час виконання лабораторних робіт; б) *наочні* – ілюстрування лекційного матеріалу таблицями, схемами та графіками; в) *практичні* – виконання практичних робіт, що передбачає організацію навчальної роботи для отримання нових знань.
Необхідне обладнання	персональний комп’ютер, операційні системи (Windows, Linux), загальновживані комп'ютерні програми, проектор
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • практичні/самостійні тощо: 80% семестрової оцінки; максимальна кількість балів 80 • контрольні заміри (модулі): 20% семестрової оцінки; максимальна кількість балів 20 Підсумкова максимальна кількість балів 100. **Додаткові бали** можна отримати за результатами неформального та/або інформального навчання по тематиці даного курсу. Визнання та зарахування результатів такого навчання відбувається у відповідності до наданих документів про неформальне та/або інформальне навчання. **Зокрема, додаткові 20 балів можна отримати за проходження онлайн курсів:** Безпека в інтернеті під час війни: практичний курс**:** https://prometheus.org.ua/prometheus-free/cybersecurity-during-war-practical/ Основи інформаційної безпеки https://prometheus.org.ua/prometheus-free/info-security-basics/ або подібних за тематикою курсів. **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. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції і лабораторні заняття 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.

	Література. Усю література, яку студенти не зможуть знайти самостійно, буде надано викладачами виключно в освітніх цілях без права її передавання третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. **Політика виставлення балів.** Враховуються бали, набрані на семінарах та поточному тестуванні. При цьому обов'язково враховуються присутність на заняттях та активність студента під час заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях, не пов'язаних із навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. **Жодні форми порушення академічної доброчесності не толеруються**.
Контрольні питання	1. Сутність поняття «інформаційний простір» та його властивості. 2. Сутність поняття «кібернетичний простір» («кіберпростір») та його властивості. 3. Сутність та визначення поняття «кібербезпека». 4. Взаємозв'язок інформаційної безпеки та кібербезпеки. 5. Ознаки коректності застосування термінів «інформаційна безпека» та «кібербезпека». 6. Становлення кібертероризму. Історичні факти. 7. Погрози безпеки інформаційних систем та їх класифікація. 8. Аналіз погроз безпеки та зловживань; оцінка привабливості погроз для порушника. 9. Класифікація вірусів, структура вірусу. 10. Вибір засобів антивірусного захисту. Загальні правила захисту. 11. Види пам'яті ПК та її захист від несанкціонованого доступу. 12. Типи і характеристики носіїв інформації та їх захист від несанкціонованого доступу. 13. Характеристика ОС, їх захист від несанкціонованого доступу. 14. Загальні відомості щодо команд захисту інформації в ОС. 15. Загальні відомості про комп'ютерні віруси і методи захисту від них. 16. Загальні відомості про архівацію файлів, методи архівації. 17. Загальні відомості про форматування дисків, методи їх форматування. 18. Методи захисту записів на дисках ПК. Диспетчер Файлів Windows, призначення; можливості роботи з панелями, дисками, каталогами, файлами. 19. Загальні відомості про редактори текстів та можливості несанкціонованого доступу до інформації на ПК. 20. Основні відомості про алгоритми захисту інформації від несанкціонованого доступу. 21. Форми використання комп'ютерної техніки та захисту її від несанкціонованого доступу. 22. Захист від несанкціонованого доступу в Windows. 23. Основні криптографічні методи. 24. Шифрування за допомогою генератора псевдовипадкових чисел. 25. Системи з відкритим ключем (RSA). 26. Системи шифрування DES.

	27. Моделі захисту інформаційних систем. 28. Механізми захисту інформації. 29. Методи захисту інформаційних систем. 30. Класифікація погроз безпеки інформаційних систем. 31. Аналіз погроз і зловживань в інформаційному просторі . 32. Кількісні та якісні показники стану захищеності інформації. 33. Сучасні антивірусні програми та їх використання. 34. Цифровий підпис при передачі даних. 35. Стандарти шифрування України. 36. Класифікація інформаційних систем (ІС). 37. Класифікація інформації щодо її значимості в соціальних відносинах: відкрита інформація, інформація з обмеженим доступом. 38. Закон України – Про інформацію – основа державно-правового регулювання соціальних інформаційних відносин в Україні. 39. Основні положення Стратегії кібербезпеки України. 40. Основні положення Закону України «Про інформацію» в частині забезпечення інформаційної безпеки. 41. Основні положення Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» в частині забезпечення інформаційної безпеки. 42. Види способів (методів) несанкціонованого доступу до інформації в інформаційних системах. 43. Алгоритм цифрового підпису. 44. Методи захисту програм від копіювання. 45. Програмні комплекси криптографічного захисту інформації. 46. Структура і захист локальних комп‘ютерних мереж в електронному офісі. 47. Організація інформаційно-аналітичної роботи щодо захисту інформації в ІС. 48. Оцінка внутрішніх та зовнішніх факторів захисту інформації в ІС. 49. Планування, визначення та організація засобів захисту інформації в інформаційних системах. 50. Алгоритми хешування. 51. Поняття електронного ключа. 52. Поняття та сутність технічного захисту інформації в інформаційних системах. 53. Стандарти цифрового підпису. 54. Система стандартизації захисту в мережах. Протоколи TCP/IP. 55. Основні компоненти архітектури безпеки INTERNET. 56. Електронна пошта. 57. Застосування методів адміністративного впливу в забезпеченні захисту інформації в ІС (система паролів, розподілений доступ, аналіз). 58. Захист в INTERNET: використання брандмауерів. 59. Тенденції, концепції та проблеми правового регулювання захисту інформації в ІС.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Таблиця 1

Схема курсу «**Основи інформаційної та кібербезпеки**»

Тиждень	Назва теми	Форма діяльності та обсяг годин	Термін виконання
1	**Тема 1. Основні положення інформаційної безпеки** Поняття інформаційної безпеки. Основні задачі інформаційної безпеки. Інформація, що підлягає захисту. Загрози інформаційної безпеки.	Лекції – 2 год., самостійна робота – 4 год.	2 тижні
2	**Тема 2. Законодавчий та адміністративний рівні інформаційної безпеки** Законодавство України в галузі інформаційної безпеки. Огляд міжнародних стандартів у галузі інформаційної безпеки.	Лекції – 2 год., самостійна робота – 4 год.	2 тижні
3	**Тема 3. Організаційний та програмно-технічний рівні інформаційної безпеки** Фізичний захист. Заходи щодо захисту локального комп'ютера. Криптографічні засоби захисту. Основні сервіси безпеки. Принципи архітектурної безпеки. Екранування. Аналіз захищеності.	Лекції – 2 год., самостійна робота – 4 год.	2 тижні
4	**Тема 4. Захист в системах передачі даних та системах зв'язку** Методи та технології захисту інформації. Оцінка захищеності інформації в системах передачі даних та системах зв'язку.	Лекції – 2 год., самостійна робота – 4 год.	2 тижні
5	**Тема 5. Захист в мережах** Засоби забезпечення безпеки в обчислювальних мережах. Захист серверів та робочих станцій. Засоби захисту локальних мереж при приєднанні до Інтернету. Технологія міжмережевих екранів. Технологія віртуальних приватних мереж.	Лекції – 2 год., самостійна робота – 4 год.	2 тижні
6	**Тема 6. Захист програм та даних** Шкідливі програмні засоби. Захист програмного забезпечення. Ідентифікація програм та захист авторських прав.	Лекції – 2 год., самостійна робота – 4 год.	2 тижні
7	**Тема 7. Захист в операційних системах** Підсистема безпеки операційної системи (Windows, Linux). Критерії захищеності операційних систем.	Лекції – 2 год., самостійна робота – 4 год.	2 тижні
8	**Тема 8. Методи і засоби соціального інжинірингу** Техніки та види атак. Методика протидії атакам типу соціального інжинірингу. Захист інформації від соціотехнічних атак.	Лекції – 2 год., самостійна робота – 4 год.	2 тижні

Таблиця 2

Теми практичних занять

Тиждень	Назва теми	Форма діяльності та обсяг годин	Термін виконання
1	Встановлення та конфігурування систем Firewall (в ОС Windows та Ubuntu).	практ. заняття – 2 год., самостійна робота – 2 год.	2 тижні
2	Дослідження криптостійкості паролів.	практ. заняття – 2 год., самостійна робота – 2 год.	2 тижні
3	Дослідження ознак присутності на комп'ютері шкідливих програм.	практ. заняття – 2 год., самостійна робота – 3 год.	2 тижні
4	Програмне відновлення вилучених файлів.	практ. заняття – 2 год., самостійна робота – 3 год.	2 тижні
5	Методи захисту інформації у автоматизованих системах.	практ. заняття – 2 год., самостійна робота – 4 год.	2 тижні
6	Методи захисту інформації у телекомунікаційних мережах та відкритих каналах зв’язку.	практ. заняття – 2 год., самостійна робота – 4 год.	2 тижні
7	Тестування мереж на проникнення. Збір інформації про web-додатки.	практ. заняття – 2 год., самостійна робота –4год.	2 тижні
8	Вивчення роботи мережевого сніфера для аналізу пакетів протоколу HTTP.	практ. заняття – 2 год., самостійна робота – 4 год.	2 тижні