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 № __ від ___ _____ 2021 р.)

Завідувач кафедри _____ І.Б. 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 2021 р.

	Силабус навчальної дисципліни **«ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ»** **Галузь знань: 05 «Соціальні та поведінкові науки»** **Спеціальність: 051 «Економіка»**
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	Моб. телефон: +38(098)-26-24-403 Електронні скриньки: an_zador@ukr.net; anna.zadorozhna@lnu.edu.ua Viber: 098-26-24-403; 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	Щочетверга, 15:00-16:20 год. (вул. Коперника, 3, ауд. 302) Консультації в день проведення лекцій/лабораторних занять (за попередньою домовленістю). Можливі онлайн консультації через Skype, Viber, Telegram. Для погодження часу он-лайн консультацій слід писати на електронну пошту викладача або дзвонити.
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	Курс розроблено таким чином, щоб надати здобувачам вищої освіти необхідні знання для набуття і прикладного використання компетентностей, обов'язкових для того, щоби стати фахівцем із застосування інформаційних технологій у різних сегментах економіки, управління й бізнесу, розробки універсальних й спеціалізованих комп'ютерних програм, умінні організовувати захист інформації від зловмисних дій, а також посісти конкурентоздатну позицію на ринку праці. Тому у курсі вивчаються методи захисту інформації від несанкціонованого доступу в інформаційних системах, способи належного зберігання інформації.
Коротка анотація дисципліни	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).

Мета та цілі дисципліни	Метою вивчення нормативної дисципліни «Захист інформації в інформаційних системах» є формування теоретичних знань щодо можливих небезпек і ступеня ризику втрат інформації, а також практичних навичок щодо забезпечення захисту програмної продукції. Основні завдання дисципліни «Захист інформації в інформаційних системах» – вивчення сучасних інформаційних технологій у галузі інформаційної безпеки та криптографічних методів захисту інформації; підготовка фахівців з розробки та впровадження технологій комп'ютерного захисту інформації, забезпечення цілісності даних, конфіденційності, контролю передачі інформації, ідентифікації, аутентифікації, криптографії, інтегрованих систем, політики безпеки, менеджменту в галузі безпеки.
Література для вивчення дисципліни	***Література:*** **Основна** 1. Бармен С. Разработка правил информационной безопасности / С. Бармен. – К.: «Вильямс», 2002. – 208 с. 2. Батюк А. С. та ін. Інформаційні системи в менеджменті: навч. посіб. / А. С. Батюк, З. П. Двуліт, К. М. Обельовська, І. М. Огородник, Л. П. Фабрі. – Львів: Національний університет «Львівська політехніка (Інформаційно-видавничий центр «Інтелект+» Інституту післядипломної освіти), «Інтелект-Захід», 2004. – 520 с. 3. Галатенко В. А. Основы информационной безопасности: курс лекций: учеб. пособ. / под ред. В. Б. Бетелина. Изд. 3-е. М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. 208 с. 4. Годин В. В., Корнеев И. К. Информационное обеспечение управленческой деятельности: учеб. / В. В. Годин, И.К. Корнеев. – М.: Мастерство; Высшая школа, 2001. – 240 с. 5. Гужва В. М. Інформаційні системи і технології на підприємствах: навч. посіб. / В. М. Гужва. – К.: КНЕУ, 2001. – 400 с. 6. Гундарь К. Ю. та ін. Защита информации в компьютерних системах / К. Ю. Гундарь, А. Ю. Гундарь, Д. А. Янишевский. – К.: «Корнійчук», 2000. – 152 с. 7. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Чинний з 29.12.2014 р. ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. – 228 с. 8. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція хешування. – Чинний з 29.12.2014 р. – ПАТ «Інститут інформаційних технологій» Мінекономрозвит-ку України, 2016. – 228 с. 9. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. К. : Держстандарт України, 2003. 10. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого

доступу. – Чинний з 28.04.1999. – К.: ДСТСЗІ СБ України, 1999. – 14 с.
11. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний з 28.04.1999. – К.: ДСТСЗІ СБ України, 1999. – 53 с.
12. Інформаційна безпека: навч. посіб. / С. В. Кавун, В. В. Носов, О. В. Манжай. Харків: Вид. ХНЕУ, 2008. – 352 с.
13. Інформаційні системи і технології в економіці / за ред. В. С. Пономаренка. – К.: ВЦ «Академія», 2002. – 544 с.
14. Кавун С. В. Информационная безопасность в бизнесе: науч. изд. Харьков: Изд. ХНЕУ, 2007. – 408 с.
15. Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Харків: ХНЕУ, 2011. – 510 с.
16. Ляшенко І.О. Європейські критерії безпеки інформаційних технологій / І.О. Ляшенко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2012. – № 1 (13). – С. 84–86.
17. Остапов С.Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с. URL: https://www.twirpx.com/file/2340575/
18. Попов В. Практикум по Internet-технологиям / В. Попов. – Санкт-Петербург.: Питер, 2002. – 480 с.
19. Про захист інформації в інформаційно-комунікаційних системах: Закон України від № 80/94ВР. Відомості Верховної Ради України. 1994. № 31. ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр
20. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. Відомості Верховної Ради України. 2017, № 45, ст. 400. URL: https://zakon.rada.gov.ua/laws /show/2155-19.
21. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
22. Токен – новий вид інформації. Газета «Інтерактивна бухгалтерія» №128 /2019. URL: https://interbuh.com.ua/ua/ documents/oneanalytics/131413
23. Хорошко В.О. Основи інформаційної безпеки: підручник / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест; за ред. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.
24. Юринець В. С., Гончарук Я. Л. Основи автоматизованих інформаційних систем: навч. посіб. / В. С. Юринець, Я. Л. Гончарук. – Л.: ЛНУ, 2001. – 256 с.

Додаткова

1. Алферов А. П. Основы криптографии: учеб. пособ. / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.
2. Басалова Г. В. Основы криптографии / Г. В. Басалова. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 283 с. URL: https://www.twirpx.com/file/1907188/
3. Воробьев С. П., Орловский Н. М. Зашита информации: учеб. пособ. / С. П. Воробьев, Н. М. Орловский. ЮРГПУ (НПИ)

	им. М. И. Платова. – Новочеркасск: ЮРГПУ(НПИ), 2015.– 27 с. 4. Вострецова Е. В. Основы информационной безопасности : учеб. пособ. / Е. В. Вострецова. – Екатеринбург : Изд-во Урал.ун-та, 2019. – 204 с. 5. Дорошенко А. Н. Информационная безопасность. Методы и средства защиты информации в компьютерных системах : учебн. пособ. / А. Н. Дорошенко, Л. Л. Ткачев. – М. : МГУПИ, 2006. – 143 с. 6. Кавун С. В. Информационная безопасность в бизнесе: науч. изд. Харьков: Изд. ХНЕУ, 2007. – 408 с. 7. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х.: ХНЕУ, 2013. – 476 с. URL: https://www.twirpx.com/file/2340575/ 8. Хорошко В. О. Основи інформаційної безпеки: підручник / В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест; за ред. В. О. Хорошка. – К.: ДУІКТ, 2008. – 186 с. ***Інтернет-джерела:*** – http://www.google.com/ – http://www.studentam.kiev.ua/ – Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України: нормативно-правова база. – Режим доступу: www.dstszi.gov.ua/dstszi/control/uk/index – http://samoychiteli.ru/documentcontents34385.html
Тривалість курсу	90 год.
Обсяг курсу	54 години аудиторних занять. З них 18 годин лекцій, 36 годин лабораторних занять та 36 годин самостійної роботи
Очікувані результати навчання	Після завершення цього курсу студент буде : **а) знати** • що собою являє політика інформаційної безпеки; • правила безпеки при роботі із комп'ютерними мережами; • мережу Інтернет та електронну пошту; • криптографічні методи захисту інформації; • будову та принципи дії комп'ютерних вірусів і шкідливих програм; **б) уміти** • встановлювати та використовувати антивірусні програми та забезпечувати безпеку використання WWW за допомогою web-браузерів; • розробляти й вирішувати актуальні питання теорії і практики інформаційної безпеки; • застосовувати знання в практичній діяльності.
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
	Проведення лекцій, лабораторних робіт та консультації для кращого розуміння тем.

	Викладання навчальної дисципліни передбачає поєднання традиційних форм аудиторного навчання з елементами електронного навчання, в якому використовуються спеціальні інформаційні технології, такі як комп'ютерна графіка, аудіо та відео, інтерактивні елементи, онлайн консультування і т.п.
Теми	Подано у формі Схеми курсу
Підсумковий контроль, форма	Екзамен в кінці семестру /комбінований (відповідь + письмовий тест). Оцінка складається із суми кількості балів, нарахованих за поточну успішність протягом семестру (здачу лабораторних робіт, виконання самостійних робіт та індивідуального завдання, написання контрольної модульної роботи) та балів, отриманих за здачу екзамену. Методи контролю: спостереження за навчальною діяльністю здобувачів вищої освіти, усне опитування, письмовий контроль, тестовий контроль, виконання навчальних та індивідуальних завдань.
Пререквізити	Навчальна дисципліна «Захист інформації в інформаційних системах» взаємопов'язана з такими дисциплінами, як «Економіко-математичне моделювання», «Інформаційні та комунікаційні технології» та ін.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентація, лекція-бесіда, лекція-візуалізація, колаборативне навчання (форми – групові проекти, спільні розробки і т. д.), проектно-орієнтоване навчання, навчальна дискусія, мозкова атака, кейс-метод, демонстрування, самостійна робота, лабораторні роботи, метод порівняння, метод узагальнення, метод конкретизації, метод виокремлення основного, обговорення, робота над помилками.
Необхідне обладнання	Вивчення курсу потребує використання загально вживаних програм і операційних систем. Мультимедійна дошка, проектор.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • лабораторні/самостійні тощо: 45% семестрової оцінки; максимальна кількість балів – 45; • контрольна робота - 5% семестрової оцінки; максимальна кількість балів –5; • екзамен: 50% семестрової оцінки (максимальна кількість балів – 50). Підсумкова максимальна кількість балів – 100. **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 практичній (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 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 робіт, передбачених курсом. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. П**олітика виставлення балів.** Враховуються бали набрані на поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час лабораторного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Питання до екзамену.	1. Загальні поняття захисту інформації. 2. Закони України про захист інформації. 3. Аналіз даних захисту. 4. Право інтелектуальної власності та політика інформаційної безпеки. 5. Управління безпекою. 6. Розробка правил безпеки. 7. Міжнародні правила застосування шифру. 8. Управління криптографією. 9. Вимоги до криптографічних систем. 10. Метод шифрування. 11. Ключ шифрування. 12. Симетричні методи шифрування. 13. Несиметричні методи шифрування. 14. Проблеми та перспективи криптографічних систем. 15. Симетричне шифрування. 16. Асиметричне шифрування та його використання. 17. Управління ключами шифрування. 18. Правовий статус електронного цифрового підпису 19. Призначення електронного підпису. 20. Необхідність сертифікації засобів ЕЦП і відкритих ключів. 21. Особливості рукописного підпису. 22. Особливості ЕЦП. 23. Поняття токенів. 24. Еліптичне шифрування інформації. 25. Загальна характеристика систем захисту в інформаційних мережах. 26. Фізична безпека. 27. Аутентифікація та безпека мережі. 28. Паролі. 29. Захист інформації в бездротових локальних мережах. 30. Криптостійкість засобів ЕЦП. 31. Поняття електронного сертифікату.

	32. Моделі систем сертифікації. 33. Проблеми та перспективи впровадження ЕЦП в Україні. 34. Користувацький інтерфейс. 35. Телекомунікації та віддалений доступ. 36. Резервне копіювання. 37. Адміністрування інформаційних систем. 38. Безпека протоколів TCP/IP; 39. Програмні засоби захисту інформації. 40. Інформаційні технології та право. 41. Комп'ютерні злочини. 42. Правила роботи з WWW. 43. Обов'язки користувача. 44. Правила використання електронної пошти. 45. Адміністрування електронної пошти. 46. Використання електронної пошти для конфіденційного обміну інформацією. 47. Комп'ютерні віруси та їх властивості. 48. Класифікація вірусів. 49. Основні види комп'ютерних вірусів та схеми їх функціонування. 50. Структура комп'ютерних вірусів. 51. Програми виявлення вірусів та заходи по захисту та профілактиці. 52. Антивірусні пакети.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Тиждень / дата / год.	Тема, план, короткі тези	Форма діяльності (заняття)	Література. Ресурси в інтернеті	Завдання, год.	Термін виконання
1	2	3	4	5	6
Тиж. 1 2 год.	Тема 1. Загальні аспекти захисту інформації. Загальні поняття захисту інформації. Закони України про захист інформації.	Лекція	Осн. [1-6, 12-17, 19-21]. Дод. [3-5]. Інт. [2-5].	Опрацювати лекційний матеріал, підготуватися до лабораторного заняття 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 1 2 год.	Тема 1. Загальні аспекти захисту інформації.	Лабораторна робота	Осн. [1-6, 12-17, 19-21]. Дод. [3-5]. Інт. [2-5].	Операції, що використовуються у криптографії. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 1 2 год.	Тема 1. Загальні аспекти захисту інформації.	Лабораторна робота	Осн. [1-6, 12-17, 19-21]. Дод. [3-5]. Інт. [2-5].	Операції, що використовуються у криптографії. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 2 2 год.	Тема 1. Загальні аспекти захисту інформації. Аналіз даних захисту. Право інтелектуальної власності та політика інформаційної безпеки. Управління безпекою. Розробка правил безпеки.	Лекція	Осн. [1-6, 12-17, 19-21]. Дод. [1-5]. Інт. [2-5].	Опрацювати лекційний матеріал, підготуватися до лабораторного заняття 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 2	Тема 1. Загальні аспекти захисту інформації.	Лабораторна робота	Осн. [1-6, 12-17, 19-21].	Робота з функціями, що	До проведення

1	2	3	4	5	6
2 год.			Дод. [3-5]. Інт. [2-5].	використовуються в теорії чисел та криптографії. 2 год.	наступного аудиторного заняття за розкладом
Тиж. 2 2 год.	Тема 1. Загальні аспекти захисту інформації.	Лабораторна робота	Осн. [1-6, 12-17, 19-21]. Дод. [3-5]. Інт. [2-5].	Робота з функціями, що використовуються в теорії чисел та криптографії. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 3 2 год.	Тема 2. Криптографічні методи захисту інформації. Міжнародні правила застосування шифру. Управління криптографією. Вимоги до криптографічних систем.	Лекція	Осн. [6-16]. Дод. [1-8]. Інт. [3-5].	Опрацювати лекційний матеріал, підготуватися до лаборатор.заняття 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 3 2 год.	Тема 2. Криптографічні методи захисту інформації.	Лабораторна робота	Осн. [6-16]. Дод. [1-8]. Інт. [3-5].	Знайомство з простими методами шифрування. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 3 2 год.	Тема 2. Криптографічні методи захисту інформації.	Лабораторна робота	Осн. [6-16]. Дод. [1-8]. Інт. [3-5].	Знайомство з простими методами шифрування. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 4 2 год.	Тема 2. Криптографічні методи захисту інформації. Класифікація криптографічних методів.	Лекція	Осн. [6-16]. Дод. [1-8]. Інт. [3-5].	Опрацювати лекційний матеріал, підготуватися до	До проведення наступного аудиторного

1	2	3	4	5	6
				лабораторного заняття 2 год.	заняття за розкладом
Тиж. 4 2 год.	Тема 2. Криптографічні методи захисту інформації.	Лабораторна робота	Осн. [1-6, 12-17, 19-21]. Дод. [3-5]. Інт. [2-5].	Знайомство з простими методами шифрування. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 4 2 год.	Тема 2. Криптографічні методи захисту інформації.	Лабораторна робота	Осн. [1-6, 12-17, 19-21]. Дод. [3-5]. Інт. [2-5].	Знайомство з простими методами шифрування. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 5 2 год.	Тема 2. Криптографічні методи захисту інформації. Проблеми та перспективи криптографічних систем. Управління ключами.	Лекція	Осн. [6-16]. Дод. [1-8]. Інт. [3-5].	Опрацювати лекційний матеріал, підготуватися до лабораторного заняття 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 5 2 год.	Тема 2. Криптографічні методи захисту інформації.	Лабораторна робота	Осн. [6-16]. Дод. [1-8]. Інт. [3-5].	Алгоритм Евкліда. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 5 2 год.	Тема 2. Криптографічні методи захисту інформації.	Лабораторна робота	Осн. [6-16]. Дод. [1-8]. Інт. [3-5].	Алгоритм Евкліда. 2 год.	До проведення наступного аудиторного

1	2	3	4	5	6
					заняття за розкладом
Тиж. 6 2 год.	Тема 2. Криптографічні методи захисту інформації. Правове, організаційне та технічне забезпечення режиму електронного цифрового підпису.	Лекція	Осн. [6-16]. Дод. [1-8]. Інт. [3-5].	Опрацювати лекційний матеріал, підготуватися до лабораторного заняття 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 6 2 год.	Тема 2. Криптографічні методи захисту інформації.	Лабораторна робота	Осн. [6-16]. Дод. [1-8]. Інт. [3-5].	Розширений метод Евкліда. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 6 2 год.	Тема 2. Криптографічні методи захисту інформації.	Лабораторна робота	Осн. [6-16]. Дод. [1-8]. Інт. [3-5].	Розширений метод Евкліда. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 7 2 год.	Тема 3. Безпека в інформаційних мережах. Фізична безпека. Загальна характеристика систем захисту в інформаційних мережах. Автентифікація та безпека мережі. Паролі. Користувацький інтерфейс. Телекомунікації та віддалений доступ. Резервне копіювання. Адміністрування інформаційних систем.	Лекція	Осн. [7-24]. Дод. [1-6]. Інт. [1-5].	Опрацювати лекційний матеріал, підготуватися до лабораторного заняття 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 7 2 год.	Тема 3. Безпека в інформаційних мережах.	Лабораторна робота	Осн. [7-24]. Дод. [1-6]. Інт. [1-5].	Симетричні методи шифрування повідомлень. 2 год.	До проведення наступного аудиторного заняття за

1	2	3	4	5	6
					розкладом
Тиж. 7 2 год.	Тема 3. Безпека в інформаційних мережах.	Лабораторна робота	Осн. [7-24]. Дод. [1-6]. Інт. [1-5].	Симетричні методи шифрування повідомлень. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 8 2 год.	Тема 4. Правила безпеки в Internet. Інформаційні технології та право. Комп'ютерні злочини. Правила роботи з WWW. Обов'язки користувача. Правила використання електронної пошти. Адміністрування електронної пошти. Використання електронної пошти для конфіденційного обміну інформацією.	Лекція	Осн. [7-24]. Дод. [1-6]. Інт. [1-5].	Опрацювати лекційний матеріал, підготуватися до лабораторного заняття 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 8 2 год.	Тема 3. Безпека в інформаційних мережах.	Лабораторна робота	Осн. [7-24]. Дод. [1-6]. Інт. [1-5].	Методи шифрування та дешифрування інформації. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 8 2 год.	Тема 3. Безпека в інформаційних мережах.	Лабораторна робота	Осн. [7-24]. Дод. [1-6]. Інт. [1-5].	Методи шифрування та дешифрування інформації. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 9 2 год.	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	Осн. [7-24]. Дод. [1-6]. Інт. [1-5].	Опрацювати лекційний матеріал, підготуватися до лабораторного заняття 2 год.	До проведення наступного аудиторного заняття за розкладом

1	2	3	4	5	6
Тиж. 9 2 год.	Тема 3. Безпека в інформаційних мережах.	Лабораторна робота	Осн. [7-24]. Дод. [1-6]. Інт. [1-5].	Методи шифрування та дешифрування інформації. 2 год.	До проведення наступного аудиторного заняття за розкладом
Тиж. 9 2 год.	Підсумковий контроль	Тестування	Осн. [1-24]. Дод. [1-8]. Інт. [1-5].	Виконання індивідуальних практ.завдань, тестових завдань	Згідно розкладу

Викладач_____ А.В. Задорожна