СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ІНФОРМАЦІЙНА БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	126 Інформаційні системи та технології
Назва освітньо-професійної програми	Інформаційні системи в економіці та бізнесі
Рівень вищої освіти	Перша(бакалаврська) вища освіта
Факультет	Факультет інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК 29 ОПП «Інформаційні системи в економіці та бізнесі»
Форма навчання	Денна

Викладач

Кононович Володимир Григорович
vl_kononovich@ukr.net

Доцент кафедри кібербезпеки та технічного захисту інформації, кандидат технічних наук, доцент.

Загальна інформація про дисципліну

Анотація до дисципліни	– Викладання дисципліни «Інформаційна безпека інформаційних» (ІБІС) є навчання базовими знаннями з проблем безпеки інформаційних систем та технологій в економіці та бізнесі, інших об’єктів інформаційних інфраструктур. У змістовних модулях розглядаються теоретичні основи та архітектурні принципи побудови системи інформаційної безпеки, забезпечення неперервної роботи організації та мінімізація розміру збитків (втрат) від подій,

	що є загрозою безпеці, шляхом їх нейтралізації. Система забезпечення інформаційної безпеки дає змогу використовувати інформацію, забезпечуючи при цьому її захист, а також захист інформаційних, електронних та комунікаційних ресурсів. Інформаційна безпека складається із трьох основних компонентів: а) конфіденційність – захист конфіденційної інформації від несанкціонованого доступу; б) цілісність – забезпечення точності та повноти інформації та комп'ютерних програм; в) доступність – забезпечення доступності інформації та необхідних послуг для користувачів. У підручнику аналізується процедура забезпечення інформаційної безпеки на основі стандартів, ISO, ДСТУ, НД ТЗІ. Державні та міжнародні стандарти сприяють розвитку суміжних видів діяльності у світі для міжнародного обміну товарами і послугами, а також розвитку співробітництва в інтелектуальній, науково-технічній та економічній сферах діяльності. .
Мета дисципліни	– Метою є формування у студентів знань і навичок з основними техніками, технологіями та механізмами інформаційної безпеки, із заходами безпеки та застосувати їх до широкого кола сучасних та майбутніх проблем з інформаційної безпеки ІС, захисту пристроїв, управлінню ключами та безпечного відновлення (виправлення). Цілі курсу полягають в ознайомленні та здобутті навиків слухачів з трьох груп вимог до системи безпеки в довільній організації. - Перша група вимог – це унікальний набір ризиків порушення безпеки, що складається із загроз інформаційним ресурсам та їх вразливостей та можливого впливу цих ризиків на функціонування організації. Ризикам можна сміливо протистояти, якщо діяти за вимогами стандартів інформаційної безпеки. Проте існують ризики, що вимагають спеціального підходу, і їх необхідно розглядати з врахуванням оцінки кожної конкретної організації чи кожного конкретного компонента інформаційної системи. - Друга група вимог – це набір правових вимог, яких має дотримуватися організація, її партнери, підрядники та постачальники послуг; у цьому разі зростає необхідність стандартизації із поширенням електронного обміну інформацією у мережах між організаціями. Правила міжнародних стандартів можуть слугувати надійною основою для визначення цих загальних вимог. - Третя група вимог – це унікальний набір принципів, цілей та вимог до оброблення інформації, який розробила організація для виробничої мети. Важливо (наприклад, для забезпечення конкурентоздатності), щоб у політиці безпеки було відображено ці вимоги, а також, щоби наявність чи відсутність засобів забезпечення безпеки в інформаційній інфраструктурі не суперечили меті виробничої діяльності організації». У практичних правилах забезпечення інформаційної безпеки наведено за можливості вичерпні рекомендації. Їх мета – слугувати довідником для визначення засобів контролю інформаційної безпеки, що існують у фінансовій сфері, промисловості та торгівлі, а, відповідно, можуть застосовуватися великими, середніми та малими організаціями.. Враховуючи зростаючу роль електронного передавання даних по мережах між організаціями, очевидною є користь від єдиного довідкового документа з систем забезпечення інформаційної безпеки. Він дає змогу встановити взаємну довіру між організаціями, що об'єднані у корпоративну мережу, їх торговими партнерами, а також становитиме

	основу для захисту інформаційних ресурсів.
Компетентності, формуванню яких сприяє дисципліна	**ЗК-3**. Здатність до розуміння предметної області та професійної діяльності. **СК-2**. Здатність застосовувати стандарти в області інформаційних систем та технологій при розробці функціональних профілів, побудові та інтеграції систем, продуктів, сервісів і елементів інфраструктури організації. **СК-5**. Здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем. **СК-6**. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків. **СК-11.** Здатність до аналізу, синтезу і оптимізації інформаційних систем та технологій з використанням математичних моделей і методів.
Результати навчання	**ПРН-9**. Здійснювати системний аналіз архітектури підприємства та його IT-інфраструктури, проводити розроблення та вдосконалення її елементної бази і структури. **ПРН-10**. Розуміти і враховувати соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії, пожежної безпеки та існуючих державних і закордонних стандартів під час формування технічних завдань та рішень.. **ПРН-15**. Знати методи захисту інформації, моделі безпеки інформаційних систем, використовувати ці знання при створенні безпечних інформаційних систем.
Обсяг дисципліни	Загальний обсяг дисципліни:4 кредити ЄКТС (120 години). Для денної форми навчання: лекції – 16 годин, лабораторні роботи – 14 годин, практичні заняття –14 годин, самостійна робота – 76 годин. Для заочної форми навчання: лекції – 6 годин, лабораторні роботи – 4 годин, практичні заняття –4 годин, самостійна робота – 106 годин.
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Дисципліна викладається у 5-му семестрі

Програма дисципліни

Тема 1.	***Теоретичні основи та архітектурні принципи побудови системи інформаційної безпеки інформаційних систем*** **Лекція 1.** Основні поняття та історичний огляд моделей захисту інформації та інформаційної безпеки. **Практичне заняття 1.** Сучасна технічна модель системи безпеки інформаційних технологій. **Лабораторна робота 1.** Організація реагування та обробки інцидентів безпеки у інформаційних системах.

	Лекція 2. Гармонізована технічна модель системи забезпечення інформаційної безпеки інформаційних технологій. **Практичне заняття 2.** Протоколи технологій ідентифікації та автентифікації. **Лабораторна робота 2.** Реалізація автоматизованої системи обробки інцидентів безпеки у інформаційних системах. **Лекція 3.** Модель авторизованої системи безпеки інформації та приватності. **Практичне заняття 3.** Технології захисту від несанкціонованої зміни програмного, системного та апаратного забезпечення. **Лабораторна робота 3.** Розробка Положення про службу захисту інформації в інформаційно-комунікаційних системах. **Лекція 4.** Моделі технологій та технік кібербезпеки. **Практичне заняття 4.** Технологія проектування систем IT-безпеки. **Лабораторна робота 4.** Розробка алгоритму і програми послуг «Ідентифікація та автентифікація».
Тема 2.	***Методи, засоби, заходи забезпечення інформаційної безпеки інформаційних систем*** **Лекція 5.** Аксіоматичні основи теорії та постулати інформаційної безпеки. **Практичне заняття 5.** Протоколи електронного цифрового підпису. **Лабораторна робота 5.** Алгоритми і програми послуги інформаційної безпеки «Повторне використання». **Лекція 6.** Надбудований комплекс заходів захисту інформації над стандартними операційними системами. **Практичне заняття 6.** Математичні методи оцінки ефективності парольного захисту. **Лабораторна робота 6.** Розробка алгоритму і програми послуги інформаційної безпеки «Реєстрація подій» **Лекція 7.** Структура організаційно-технічної моделі кіберзахисту. **Практичне заняття 7.** Протоколи контролю цілісності. **Лабораторна робота 7.** Послуга перевірки послуг безпеки «Адміністративна цілісність». **Лекція 8.** Соціальна інженерія як складова кібернетичних атак і частина системи безпеки інформації **Самостійна робота 1.** Порядок впровадження авторизованої системи безпеки інформації, інформаційної системи та приватності **Самостійна робота 2.** Порядок впровадження авторизованих заходів безпеки інформації, інформаційної системи та приватності **Самостійна робота 3.** Криптографічні протоколи: основні властивості та вразливості. **Самостійна робота 4.** Комплексна система інформаційної безпеки центру обробки викликів органу внутрішніх справ.

Список рекомендованих джерел

1. Інформаційна безпека інформаційних систем: підручник / Кононович В.Г. / за заг. ред. проф. В. В. Корчинського. Одеса: ДУІТЗ. 2024. 211 с..
2. Кононович В. Г., Стайкуца С. В., Бердніков О. М., Севастєєв Є. О., Швець О. В. Інформаційна безпека інноваційної діяльності в інфокомунікаціях : підручник та дистанційний практикум. Одеса: ДУІТЗ, 2023. 298 с
3. Вараксин О.О. Кібербезпека мереж наступного покоління : навч. посібник / О.О. Вараксин, Є.В. Василиу, С.М. Горохов , В.Й. Кільдишев, В.Г Кононович ; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ, – 2013. – 240 с.

4. Голев Д.В. Методики оцінки інформаційної захищеності телекомунікацій: навч. посібник / Д.В. Голев, В.Г. Кононович, С.В. Хомич ; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ, – 2013. – 218 с.
5. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення.
6. ДСТУ 7731:2015 «Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, MOD)».
7. ДСТУ ISO 15408-1: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 1. Вступ і загальна модель (ISO/IEC 15408:2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 1: Introduction and general model).
8. ДСТУ ISO/IEC 15408-2: 2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 2: Security functional requirements.
9. ДСТУ ISO/IEC 15408-3: 2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 3: Security assurance requirements.
10. ДСТУ ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management.
11. ДСТУ ISO/IEC 27032:2016. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки [Електронний ресурс]. – Київ: ДП «УкрНДНЦ», 2018. – Режим доступу до ресурсу: http://cyberrus.com/wp-content/uploads/2014/03/28-35.pdf
12. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” №2594-IV від 31.05.2006. – 3 с.
13. Закон України «Про критичну інфраструктуру».
14. Кононович В.Г. Контури систем забезпечення кібербезпеки цифровізованого суспільства та кібернетизованого виробництва, бізнесу й управління. /В.Г. Кононович, С.В. Стайкуца, І.В. Кононович, М.Г. Романюков // «Перспективні напрями захисту інформації : Матеріали шостої міжнародної всеукраїнської наук. пр. конф.», тези доповідей. – м. Одеса, 02-06 вересня 2020 р. – Одеса, Бондаренко М.О. ОНАЗ, 2020. – С. 70-75.
15. Інформаційна безпека цифрових програмно-керованих АТС : [навч. посіб.] / С.М. Горохов, В.Г. Кононович, С.В. Стайкуца, Т.М. Лемеха, Ю.В. Копитін; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 244 с.
16. Кононович В. Г., Стайкуца С. В., Берднiков О. М., Севастєєв Є. О., Швець О. В. Інформаційна безпека інноваційної діяльності в інфокомунікаціях : підручник та дистанційний практикум. / За ред. д.т.н., проф. В. В. Корчинського. Передмова д.т.н., проф. Є. В. Василіу. Післямова д.т.н., проф. С. О. Гнатюка. Одеса: ДУІТЗ, 2023. 298 с.
17. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 3. Архітектура безпеки Концепція захисту інформації: Навч. посібник Затверджено Міністерством транспорту та зв’язку України. – Одеса: ОНАЗ, – 2009. – 194 с.
18. Копитін Ю.В. Модель страхування ризиків інформаційної безпеки./ Копитін Ю.В. // Цифрові технології. – 2010№ 8. [Електронний ресурс]. – Режим доступу: http://digitech.onat.edu.ua/files/13.pdf.
19. Методики категоризації об’єктів критичної інфраструктури, затвердженої постановою Кабінету Міністрів України від 09 жовтня 2020 року №

1109.
20. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
21. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
22. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затв. наказом ДСТСЗІ СБУ від 04.12.2000 р. № 53. – 26 с.
23. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Режим доступу: http://www.dsszzi.gov.ua/ dstszi/control/uk/publish/article?art_id=40381&cat_id=38835.
24. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. – Режим доступу: http://www.dsszzi.gov.ua/ dstszi/control/uk/publish/article?art_id=40342&cat_id=38835
25. НД ТЗІ 3.6-004-21 «Порядок впровадження систем безпеки інформації в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці».
26. НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації»;
27. НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»
28. НД ТЗІ 3.6-007-21 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».
29. Обеспечение целостности программного обеспечения Cisco IOS. [Электронный ресурс] (Назва з екрану) – URL: https://www.cisco.com/c/dam/global/ru_ru/about/brochures/assets/pdfs/cisco_ios_software_integrity_assurance.pdf (– Дата звернення: 05.02.2021).
30. Офіційний інтернет-сайт Державної служби спеціальних телекомунікаційних систем та захисту інформації. Електронний ресурс: «Біла книга Держспецзв'язку». http://www.dstszi.gov.ua/dstszi - 47 с.
31. Соціальна інженерія (системний аналіз): навч. посіб. / [В.М.Петрик, В.І.Курганевич, В.Г.Кононович та ін.] / за заг. ред. В.І.Курганевича та В.М.Петрика – К., 2019. – 200 с.
32. Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Затв. постановою КМУ від 16.11.2002 р. №1772. Із змінами, внесеними згідно з Постановою КМУ від 08.12.2006 р. № 1700. – 2 с.
33. Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 94 від 10.06.2008. – 5 с.
34. Постанова КМУ від 29.06.2004 р. № 812. Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану.
35. Постанова Кабінету Міністрів України № 943 від 09.10.2020 р.
36. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджено

постановою Кабінету Міністрів України від 29 березня 2006 р. № 373. – С 12.
37. Правила посиленої сертифікації [Електронний документ] / Наказ ДСТСЗИ від 13.01.2005 №3. – URL: https://zakon.rada.gov.ua/laws/show/992-2018-%D0%BF#n13.
38. Про електронні довірчі послуги / Закон України [Електронний документ] // Відомості Верховної Ради (ВВР), 2017, № 45, ст.400. – URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (Дата звернення: 21.02.2021).
39. Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг / Постанова КМУ від 7 листопада 2018 р. № 992 Київ [Електронний документ]. – URL: https://zakon.rada.gov.ua/laws/show/992-2018-%D0%BF#n13.
40. Рекомендація **МСЭ-Т** Y. 2001. Глобальна інформаційна інфраструктура. Загальний огляд мереж наступного покоління (NGN).
41. Рекомендація **МСЭ-Т** Y. 2011. Глобальна інформаційна інфраструктура. Загальні принципи і основні поняття моделі для мереж наступного покоління.
42. Рекомендація ITU-T Y.3302. Future networks. Functional architecture of software-defined networking.
43. СОУ Н НБУ 65.1 СУІБ 2.0:2010 Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою:. – К.: Національний банк України, 2010. – 209 с.
44. Тардаскін М.Ф., Кононович В.Г. Технічний захист комерційної таємниці підприємства зв'язку: Навч. посібник/ За ред. М.В. Захарченка. – Одеса: ОНАЗ, 2002. – 76 с.
45. Тардаскіна Т.М. Менеджмент інформаційної безпеки в галузі зв'язку: навч. посіб./ Т.М. Тардаскіна, В.Г. Кононович – Одеса: ОНАЗ ім. О.С. Попова, 2010. – 268 с.
46. M800 CDMA Mobile Switching Centre System Description – working documents
47. Clark J., Jacob J. A Survey of Authentication Protocol Literature: Version 1.0. 17 Nov. 1997. http://www.cs.york.ac.uk/ jac/papers/drareview.ps.gz, 1997.
48. Cremers C. J. F., Lafourcade P. Comparing State Spaces in Automatic Security Protocol Verification. ETH Technical Report. 2007. No. 558. 26 p.
49. Index of the security protocols repository (SPORE) // Laboratorie Sp´ecification et V´erification. http://www.lsv.ens-cachan.fr/spore/table.html.
50. ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements.
51. ISO/IEC 27003:2010 «Information technology – Security techniques – Information security management system implementation guidance» (Настанова з впровадження системи управління інформаційною безпекою).
52. ISO/IEC TR 18044:2004. Information technology - Security techniques - Information security incident management.

1. Інформаційні ресурси

1. http://www.dut.edu.ua/uploads/1_49183247.pdf .
2. http://www.dut.edu.ua/uploads/1_1066_65357958.pdf .
3. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835
4. http://shop.uas.org.ua/ua/katalog-normativnih-dokumentiv/35-informatsiyni-tekhnolohiyi-kontorski-mashyny/informacijni-tehnologii-metodi-zahistu-

osnovni-polozhennja-schodo-zabezpechennja-nevtruchannja-v-osobiste-zhittja.html .
5. http://www.avispa-project.org .
6. https://www.dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798
7. https://www.iso.org .
8. https://www.pdfdrive.com .
9. http://www.virtualbox.org .

Інформація про консультації

Щопонеділка у протягом семестру з 11^{50} до 13^{10}год., ауд. 205 ДУІТЗ – доц. В. Г. Кононович

Загальна схема оцінювання

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Шкала ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td><td rowspan="3">Нараховування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="2">Оцінювання знань здобувачів фахової передвищої освіти здійснюється за 100-бальною шкалою і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань, лабораторних та контрольних робіт) та за результати заліку/екзамену)</td></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>Незадовільно з можливістю повторного складання</td><td>Не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>Незадовільно з обов’язковим повторним вивченням дисципліни</td><td>Не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

Політика опанування дисципліни

Відвідування: Здобувачі фахової перед вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на лабораторних роботах, практичних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.
Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем фахової перед вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **myPlag.**
Умови зарахування пропущених занять:
Інші умови: Загальна оцінка з дисципліни – максимум 100 балів. У випадку отримання менше 60 балів, здобувач обов'язково здійснює перескладання для ліквідації академічної заборгованості.