МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

кафедра протидії кіберзлочинності, факультет № 4

МЕТОДИЧНІ МАТЕРІАЛИ

до практичних занять

з навчальної дисципліни **Стандартизація і сертифікація в галузі інформаційної безпеки**

обов'язкових компонент освітньої програми другого рівня вищої освіти 125 Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 16.08.2023 № 8

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри протидії кіберзлочинності (*протокол від 15.08.2023 № 19*

Розробник:
Завідувач кафедри протидії кіберзлочинності, к.ю.н., професор Манжай О.В.

Рецензенти:

Тулупов В.В., доцент кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ к.т.н., доцент;

Павликівський В.І., перший проректор Харківського університету, д.ю.н., професор

1. Розподіл часу навчальної дисципліни за темами

(денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2							
Тема № 1 **Нормативно-методична база побудови комплексної системи захисту інформації та системи управління інформаційною безпекою**	**70**	**4**	**0**	**4**	**0**	**62**	**Екзамен**
Тема № 2 **Особливості побудови системи управління інформаційною безпекою**	**110**	**26**	**0**	**26**	**0**	**58**	
Всього за семестр № 2:	**180**	**30**	**0**	**30**	**0**	**120**	

(заочна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2							
Тема № 1 **Нормативно-методична база побудови комплексної системи захисту інформації та системи управління інформаційною безпекою**	**86**	**2**	**0**	**2**	**0**	**82**	**Екзамен**
Тема № 2 **Особливості побудови системи управління інформаційною безпекою**	**94**	**4**	**0**	**8**	**0**	**82**	
Всього за семестр № 2:	**180**	**6**	**0**	**10**	**0**	**164**	

2. Методичні вказівки до практичного навчання

Тема № 1. Нормативно-методична база побудови комплексної системи захисту інформації та системи управління інформаційною безпекою

Практичне заняття «Організаційі аспекти побудови комплексної системи захисту інформації та системи управління інформаційною безпекою»

Навчальна мета заняття: отримати практичні навички пошуку та аналізу даних, необхідних для оцінки витрат і часу на побудову комплексної системи захисту інформації та системи управління інформаційною безпекою.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет»

Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (10 хв.).
3. Запропонувати механізм визначення вартості створення комплексної системи захисту інформації та системи управління інформаційною безпекою для типового підрозділу та навести орієнтовну обґрунтовану вартість робіт для кожного випадку.
4. Викладач оцінює якість роботи за чотирьохбальною шкалою.
5. По закінченні заняття підбиваються підсумки (10 хв.).

Тема № 2. Особливості побудови системи управління інформаційною безпекою

Практичне заняття «Політика безпеки»

Навчальна мета заняття: навчитися складати політику безпеки для типової організації.

Час проведення: 4 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome».

Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (10 хв.).
3. Скласти політику безпеки для типової організації з урахуванням наведених в лекційному курсі вимог. Представити її у вигляді фрагменту за одним з напрямів:
   1) контроль доступу;
   2) фізична безпека;
   3) резервне копіювання;
   4) захист від шкідливого коду;
   5) криптографічні засоби безпеки;
   6) безпека комунікацій;
   7) захист персональних ідентифікаційних даних.
4. Викладач оцінює якість роботи за чотирьохбальною шкалою.
5. По закінченні заняття підбиваються підсумки (10 хв.).

Практичне заняття «Організація побудови системи управління інформаційною безпекою»

Навчальна мета заняття: навчитися визначати права і обов'язки суб'єктів забезпечення системи управління інформаційною безпекою та оцінювати її відповідність стандартам безпеки .

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі «Інтернет».

Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (10 хв.).
3. Визначити права та обов'язки керівника організації щодо забезпечення режиму безпеки інформації.
4. Оцінити, наскільки підрозділ відповідає стандарту ДСТУ ISO/IEC 27001:2015, та що потрібно для досягнення відповідності (is.gd/oyt6l8, is.gd/hinvAo).
5. Викладач оцінює якість роботи за чотирьохбальною шкалою.
6. По закінченні заняття підбиваються підсумки (10 хв.).

Практичне заняття «Перевірка кандидата на посаду»

Навчальна мета заняття: навчитися збирати базову інформацію з відкритих джерел під час прийому на роботу.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome».

Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (10 хв.).
3. Кандидат на посаду залишив контактну адресу cyberhygieneukraine@gmail.com. Знайдіть фото, прив'язане до облікового запису та місця, які володілець облікового запису відмітив на карті. Знайдіть принаймні три ресурси, на яких під час реєстрації використовувалася встановлена електронна пошта. Встановіть, чи справжнє фото використав кандидат у своєму профілі.
4. Викладач оцінює якість роботи за чотирьохбальною шкалою.
5. По закінченні заняття підбиваються підсумки (10 хв.).

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Манжай О.В., Мелешко Д.Г., Носов В.В., Самойлов С.В. Розробка та впровадження системи управління безпекою інформації. Київ: ВАІТЕ, 2021. 138 с.

2. Манжай О. В., Манжай І. А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с. з іл.

3. Науково-практичний коментар Закону України «Про основні засади забезпечення кібербезпеки України». Станом на 1 січня 2019 року / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

Допоміжна

4. Про інформацію. Закон України від 02.10.1992, № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

5. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України: від 23.02.2006, № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

6. Про захист інформації в інформаційно-комунікаційних системах. Закон України: від 05.07.1994, № 1170-VII. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

7. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 10.08.2022).

8. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017, № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text

9. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11 березня 2021 року, введено в дію Указом Президента України від 19 березня 2021 року № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text

10. 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

11. Про захист персональних даних. Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

12. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів - На заміну ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT).

13. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) / Поправка № 2:2019.

14. (ISO/IEC 27001:2013/Cor 2:2015, IDT) Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.

15. ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) / Поправка № 2:2019 (ISO/IEC 27002:2013/Cor 2:2015, IDT). Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.

16. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT).

17. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT).

18. ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки - На заміну ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT).

19. ДСТУ ISO/IEC 27006:2015 Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2015, IDT).

20. ДСТУ ISO/IEC 27007:2018 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою (ISO/IEC 27007:2017, IDT).

21. ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки - На заміну ДСТУ ISO/IEC TR 27008:2018 (ISO/IEC TR 27008:2011, IDT).

22. ДСТУ ISO/IEC 27009:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги (ISO/IEC 27009:2016, IDT).

23. ДСТУ ISO/IEC 27017:2017 Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (ISO/IEC 27017:2015, IDT).

24. ДСТУ ISO/IEC 27021:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги до компетенції для професіоналів з керування інформаційною безпекою (ISO/IEC 27021:2017, IDT).

25. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).

26. ДСТУ ISO/IEC 27033-1:2017 Інформаційні технології. Методи захисту. Захист мережі. Частина 1. Огляд і поняття (ISO/IEC 27033-1:2015, IDT).

27. ДСТУ ISO/IEC 27033-2:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 2. Настанови щодо проектування та реалізації безпеки мережі (ISO/IEC 27033-2:2012, IDT).

28. ДСТУ ISO/IEC 27033-3:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 3. Еталонні мережеві сценарії. Загрози, методи проектування та проблеми керування (ISO/IEC 27033-3:2010, IDT).

29. ДСТУ ISO/IEC 27033-4:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 4. Убезпечення комунікацій між мережами з використанням шлюзів безпеки (ISO/IEC 27033-4:2014, IDT).

30. ДСТУ ISO/IEC 27033-5:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 5. Убезпечення комунікацій уздовж мереж із використанням віртуальних приватних мереж (VPNs) (ISO/IEC 27033-5:2013, IDT).

31. ДСТУ ISO/IEC 27033-6:2018 Інформаційні технології. Методи захисту. Безпека мережі. Частина 6. Забезпечення безпроводового доступу до IP-мережі (ISO/IEC 27033-6:2016, IDT).

32. ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами (ISO/IEC 27035-1:2016, IDT).

33. ДСТУ ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2016, IDT).

34. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT).

35. ДСТУ ISO/IEC 27038:2018 Інформаційні технології. Методи захисту. Специфікація для цифрового редагування (ISO/IEC 27038:2014, IDT).

36. ДСТУ ISO/IEC 27040:2016 Інформаційні технології. Методи захисту. Безпека зберігання (ISO/IEC 27040:2015, IDT).

37. ДСТУ ISO/IEC 27041:2016 Інформаційні технології. Методи захисту. Настанова щодо забезпечення прийнятності та адекватності методів розслідування (ISO/IEC 27041:2015, IDT).

38. ДСТУ ISO/IEC 27042:2016 Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу (ISO/IEC 27042:2015, IDT).

39. ДСТУ ISO/IEC 27043:2016 Інформаційні технології. Методи захисту. Принципи та процеси розслідування інцидентів (ISO/IEC 27043:2015, IDT).

40. ДСТУ ISO/IEC 27050-1:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 1. Огляд та поняття (ISO/IEC 27050-1:2016, IDT).

41. ДСТУ ISO/IEC 27050-3:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 3. Звід правил для електронного виявлення (ISO/IEC 27050-3:2017, IDT).

42. ДСТУ ISO/IEC 18033-1:2017 Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 1. Загальні положення (ISO/IEC 18033-1:2015, IDT).

43. ДСТУ ISO/IEC 9796-3:2015 Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі (ISO/IEC 9796-3:2006, IDT).

44. ДСТУ ISO/IEC 11770-1:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Основні положення (ISO/IEC 11770-1:2010).

45. ДСТУ ISO/IEC 11770-2:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів (ISO/IEC 11770-2:2008; Cor 1:2009, IDT).

46. ДСТУ ISO/IEC 11770-3:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів (ISO/IEC 11770-3:2008; Cor 1:2009, IDT).

47. ДСТУ ISO/IEC 11770-4:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, засновані на нестійких секретах (ISO/IEC 11770-4:2008; Cor 1:2009, IDT).

48. ДСТУ ISO/IEC 11770-5:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 5. Керування груповими ключами (ISO/IEC 11770-5:2011, IDT).

Інформаційні ресурси в Інтернеті

49. Каталог національних стандартів та кодексів усталеної практики. URL: https://katalog.uas.org.ua.