СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ЛІЦЕНЗУВАННЯ, АТЕСТАЦІЯ, СЕРТИФІКАЦІЯ В СФЕРІ БЕЗПЕКИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ »

Ступінь освіти	магістр
Галузі знань	12 Інформаційні технології 17 Електроніка, автоматизація та електронні комунікації
Тривалість викладання	3, 4 чверть
Заняття:	Весняний семестр
лекції:	2 години
практичні заняття:	1 години
Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»:
https://do.nmu.org.ua/course/view.php?id=5384

Кафедра, що викладає Кафедра безпеки інформації та телекомунікацій

Викладач:

Кручінін Олександр Володимирович

Старший викладач кафедри безпеки інформації та телекомунікацій

Персональна сторінка

https://bit.nmu.org.ua/ua/pro_kaf/prepods/kruchinin.php

E-mail:

kruchinin.o.v@nmu.one

1. Анотація до курсу

Питання, що розглядаються: Нормативно-правове забезпечення, що регламентує проведення ліцензування, атестації та сертифікації в сфері інформаційної безпеки об'єктів інформаційної діяльності, вимоги щодо провадження ліцензованої діяльності в галузі

криптографічного та технічного захисту інформації, загальні положення та порядок організації та проведення атестації комплексів технічного захисту інформації, етапи підготовки та проведення сертифікації засобів технічного та криптографічного захисту інформації . Методичні рекомендації для самостійної роботи студентів освітньо-кваліфікаційного рівня магістр спеціальності Кібербезпека.

2. Мета та завдання курсу

Мета дисципліни – формування компетентностей щодо проведення ліцензування, атестації та сертифікації в сфері інформаційної безпеки об'єктів інформаційної діяльності.

Завдання курсу:

Вивчення дисципліни має прищепити студентам системний підхід з дотриманням нормативно-правових вимог до проведення процедур, пов'язаних з ліцензуванням, атестацією та сертифікацією в сфері інформаційної безпеки об'єктів інформаційної діяльності.

3. Результати навчання

Вміти проводити необхідні дії щодо ліцензування, атестації та сертифікації діяльності в сфері інформаційної безпеки об'єктів інформаційної діяльності; бути ознайомленими з нормативно-правовим забезпеченням, що регламентує проведення процедур ліцензування, атестації та сертифікації в сфері інформаційної безпеки об'єктів інформаційної діяльності, вимогами щодо провадження ліцензованої діяльності в галузі криптографічного та технічного захисту інформації.

4. Структура курсу

ЛЕКЦІЇ 60

І. Основні визначення в сфері інформаційної безпеки об'єктів інформаційної діяльності. Нормативно-правове забезпечення щодо проведення ліцензування, атестації та сертифікації в сфері інформаційної безпеки об'єктів інформаційної діяльності

1. Об'єкт інформаційної діяльності. Термінологічна база та визначення в сфері безпеки об'єктів інформаційної діяльності.

2. Базове нормативно-правове забезпечення ліцензування, атестації та сертифікації в сфері інформаційної безпеки об'єктів інформаційної діяльності.

ІІ. Провадження ліцензованої діяльності в галузі криптографічного та технічного захисту інформації

3. Загальні положення щодо ліцензування. Термінологічна база.

4. Сутність вимог при провадженні ліцензованої діяльності в галузі криптографічного та технічного захисту інформації.

5. Заява на одержання ліцензії. Перелік та вміст документів до заяви.

III. Атестація комплексів технічного захисту інформації

6. Загальні положення щодо атестації комплексів технічного захисту інформації.

7. Порядок організації та проведення атестації.

8. Основні складові Акту атестації.

9. Засоби загального призначення, які дозволені для забезпечення ТЗІ, необхідність охорони якої визначена законодавством України.

IV. Сертифікація засобів криптографічного та технічного захисту інформації

10. Сутність і зміст загальних положень щодо процедури сертифікації.

11. Основні принципи, загальні правила, організаційна структура Української державної системи сертифікації продукції - системи сертифікації УкрСЕПРО.

12. Порядок підготовки та проведення сертифікації засобів криптографічного захисту інформації.

13.Порядок підготовки та проведення сертифікації засобів технічного захисту інформації загального призначення.

ПРАКТИЧНІ ЗАНЯТТЯ 60

I. Основні визначення в сфері інформаційної безпеки об’єктів інформаційної діяльності. Нормативно-правове забезпечення щодо проведення ліцензування, атестації та сертифікації в сфері інформаційної безпеки об’єктів інформаційної діяльності

1. Змістовий аналіз нормативно-правового забезпечення, що регламентує проведення ліцензування, атестації та сертифікації в сфері інформаційної безпеки ОІД.

II. Провадження ліцензованої діяльності в галузі криптографічного та технічного захисту інформації

2. Розробка комплекту документів до заяви про надання ліцензії на надання послуг в галузі криптографічного захисту інформації.

3. Розробка комплекту документів до заяви про надання ліцензії на надання послуг в галузі технічного захисту інформації.

III. Атестація комплексів технічного захисту інформації

4. Розробка Акту атестації КТЗІ.

IV. Сертифікація засобів криптографічного та технічного захисту інформації

5. Етапи проведення сертифікації засобів криптографічного захисту інформації.

6. Етапи проведення сертифікації засобів технічного захисту інформації загального призначення

РАЗОМ 120

5. Технічне обладнання та/або програмне забезпечення

Технічні засоби навчання: мультимедійні та комп'ютерні пристрої.

Програмні засоби дистанційної освіти: MS Office 365, MS Teams, дистанційна платформа Moodle.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74 - 89	добре
60 - 73	задовільно
0 - 59	незадовільно

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Практична частина		Бонус	**Разом**
	При своєчасному складанні	При несвоєчасному складанні		
55	40	30	5	**100**

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи. Теоретична частина оцінюється за результатами здачі іспиту. Кожний білет містить 2 питання.

6.3. Критерії оцінювання підсумкової роботи

Робота повинна містити розгорнуті відповіді на два питання білету. Якщо робота виконується у дистанційному режимі, то видача номеру білета проходить через систему MS Teams у зазначеній викладачем групі спілкування. В такому режимі виконана робота пишеться вручну, фотографується та відсилається не

електронну пошту викладача у впродовж встановленого викладачем часу. За виконану роботу нараховуються бали:

55 бали – дана розгорнута відповідь на два питання;

40 балів – дана розгорнута відповідь на одне питання, але є помилки при розгляді іншого питання, або є несуттєві помилки у відповідях на два питання;

25 балів – дана повна відповідь на одне питання або на два питання зі значними помилками;

15 балів – відповідь на одне питання із значними помилками;

0 балів – відповіді на питання відсутні або повністю невірні, або робота здана несвоєчасно.

6.4. Критерії оцінювання практичної роботи

З кожної практичної роботи здобувач вищої освіти отримує запитання з переліку контрольних запитань до роботи.

10 балів – Достатня зрозумілість відповіді

7 бали – Добра зрозумілість відповіді

4 бали – Задовільна зрозумілість відповіді

0 балів – Незадовільна зрозумілість відповіді

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". https://cutt.ly/lBesJEc.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

7.6. Бонуси

Наприкінці вивчення курсу та перед початком сесії здобувача вищої освіти буде запропоновано анонімно заповнити електронні анкети (Microsoft Forms Office 365), які буде розіслано на ваші університетські поштові скриньки. Заповнення анкет є важливою складовою вашої навчальної активності, що дозволить оцінити дієвість застосованих методів викладання та врахувати ваші пропозиції стосовно покращення змісту навчальної дисципліни. За участь у анкетуванні здобувач вищої освіти отримує 5 балів.

8 Рекомендовані джерела інформації

8.1. Нормативна

1. Закон України „Про Державну службу спеціального зв'язку та захисту інформації України".
2. Закон України „Про інформацію".
3. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах".
4. Закон України „Про основні засади державного нагляду (контролю) у сфері господарської діяльності".
5. Закон України „Про наукову і науково-технічну експертизу".
6. Положення про технічний захист інформації в Україні. Указ Президента України від 27.09.1999 № 1229.
7. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України. Указ Президента України від 30.06.2011 № 717/2011.
8. Концепція технічного захисту інформації в Україні. Постанова КМ України від 08.10.1997 № 1126.
9. Про деякі питання захисту інформації, охорона якої забезпечується державою. Постанова КМ України від 13.03.2002 № 281.
10. Положення про державний контроль за станом технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 87, зареєстрований в Міністерстві юстиції України 10.07.2007 за № 785/14052.
11. Перелік обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних. Постанова КМ України від 04.02.1998 № 121.

12. Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Постанова КМ України від 16.02.1998 № 180.
13. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Постанова КМ України від 16.11.2002 № 1772.
14. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова КМ України від 29.03.2006 № 373.
15. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
16. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
17. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
18. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
19. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.
20. ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.
21. ДСТУ 1.5:2003 Правила побудови, викладання, оформлення та вимоги до змісту нормативних документів.
22. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.
23. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
24. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
25. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 04.12.2000 № 53.
26. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці”, затверджене наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215
27. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
28. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
29. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

30. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 20.12.2000 № 60.
31. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
32. НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2, затверджений наказом ДСТСЗІ СБ України від 13.12.2002 № 84.
33. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 02.04.2003 № 33.
34. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95), затверджені наказом Державної служби України з питань технічного захисту інформації від 09.06.1995 № 25.
35. НД ТЗІ 2.7-011-2012 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.
36. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ-ПЕМВН-95), затверджені наказом Державної служби України з питань технічного захисту інформації від 09.06.1995 № 25.
37. Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від 26.03.2007 № 45, зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587.
38. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Наказ Адміністрації Держспецзв'язку від 02.12.2014 № 660 зареєстрований в Міністерстві юстиції Українит28 січня 2015 р. за № 90/26535.
39. Положення про державну експертизу в сфері технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від16.05.2007 № 93, зареєстрований в Міністерстві юстиції України 16.07.2007 за № 820/14087 із змінами, затвердженими наказом Адміністрації Держспецзв'язку від 10.10.2012 № 567, зареєстрованим в Міністерстві юстиції України 06.11.2012 за № 1863/22175.
40. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб, затверджене наказом ДСТСЗІ СБ України від 23.02.2002 № 9, зареєстрованим в Міністерстві юстиції України 13.03.2002 за № 245/6533.
41. Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що

визначається Кабінетом Міністрів України. Постанова КМ України від 16 листопада 2016 р. № 821
42. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. Наказ ДСТСЗІ СБ України від 23.02.2002 № 9, зареєстрований в Міністерстві юстиції України 13.03.2002 за №245/6533.
43. Ліцензійні умови провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України Затверджена Постановою КМ України від 16 листопада 2016 р. № 821
44. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.
45. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
46. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
47. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію. Постанова КМ України від 19 жовтня 2016 р. № 736.

8.2. Інформаційні ресурси

1. Державна служба спеціального зв’язку та захисту інформації України. – Спосіб доступу: URL: https://cip.gov.ua. – Нормативні документи
2. Верховна Рада України. – Спосіб доступу: URL: rada.gov.ua. – Нормативні документи