СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

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

Ступінь освіти	магістр
Галузь знань	12 Інформаційні технології
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/IBesJEc.

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

1. Богуш В.М., Юдін О.К. Інформаційна безпека держави. – К. : «МК-Прес». 2005. – 432с.
2. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко О.В., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.
3. НД ТЗІ 2.1-001-2001. Створення комплексів ТЗІ. Атестація комплексів ТЗІ. Основні положення.
4. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів ТЗІ від НСД та КСЗІ в ІТС.
5. НД ТЗІ 1.1-005-2007 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення (із змінами згідно наказу Адміністрації Держспецзв'язку від 03.11.2011 № 93/ДСК)
6. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.
7. НД ТЗІ 2.1-002-2007 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення
8. Математичні основи криптографії: Навч. посібник / Г.В. Кузнецов, В.В Фомичов, С.О. Сушко, Л.Я. Фомичова. – Дніпропетровськ. Національний гірничий університет, 2004. – Ч.1– 391 с.
9. Грайворонський М.В.,. Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.
10. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
11. ДСТУ ISO/IEC 27006:2008 «Інформаційні технології. Методи і засоби забезпечення безпеки. Вимоги до органів, які забезпечують аудит і сертифікацію систем менеджменту ІБ».