СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Стандартизація, сертифікація засобів та комплексів захисту інформації
Мова викладання	українська
Викладач (-і)	Ткач Ю.М., завідувач кафедри кібербезпеки та математичного моделювання, д.пед.н., доцент
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ ORCID 0000-0002-8565-0525
Контакти викладача	(063) 594 22 94 tkachym79@gmail.com

1. **Анотація курсу** -

В даний час набули широкого поширення засоби і методи несанкціонованого доступу і отримання інформації в кіберпросторі. Вони знаходять все більше застосування не тільки в діяльності державних правоохоронних органів розвинених держав, а й в діяльності хакерів і різного роду злочинних кіберугрупувань.

Необхідно пам'ятати, що природні канали витоку інформації утворюються спонтанно, в силу специфічних обставин, що склалися на об'єкті захисту. Що стосується штучних каналів витоку інформації, то вони створюються навмисно із застосуванням активних методів і способів отримання інформації. Активні способи припускають навмисне створення технічних каналів витоку інформації з використанням спеціальних технічних засобів. До них можна віднести незаконне підключення до каналів, проводам і лініям зв'язку, високочастотне нав'язування і опромінення, установка в технічних засобах і приміщеннях відеокамер, мікрофонів і телефонних закладних пристроїв, а також несанкціонований доступ до інформації, що обробляється в автоматизованих системах тощо.

Тому особливу роль і місце в діяльності по захисту інформації займають заходи щодо створення комплексного захисту, що враховують загрози національній і міжнародній безпеці і стабільності, в тому числі суспільству, особистості, державі, демократичних цінностей і суспільних інститутів, суверенітету, економіці, фінансовим установам, розвитку держави.

Змістовий модуль 1. Нормативно-правове забезпечення в сфері інформаційної безпеки

Тема 1. Структура законодавства Україні в області ІБ. Основні Закони.

Система правових та законодавчих документів, що регламентують питання ІБ. Правовий захист інформації. Структура правового законодавства. Загальний зміст організацій правового забезпечення ІБ. Структура системи стандартизації в України. Загальний її зміст.

Закон України «Про інформацію». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закон України «Про державну таємницю». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Тема 2. Закони України щодо забезпечення ІБ.

Закони України щодо забезпечення ІБ в мережах зв'язку:

Закон України «Про основи національної безпеки». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закон України «Про захист інформації в інформаційно-телекоммунікаційних системах». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закон України «Про Державну службу спеціального зв'язку та захисту інформації». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закон України «Про зв'язок». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закон України «Про моніторинг телекоммунікацій». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закон України «Про Національну систему конфіденційного зв'язку». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закони України щодо системи забезпечення безпеки. Закони України про електронний документообіг:

Закон України «Про Службу безпеки України». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закон України «Про розвідувальні органи України». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закон України «Про контррозвідувальну діяльність». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закон України «Про оперативно-розшукову діяльність». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закон України «Про електронний цифровий підпис». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Закон України «Про електронні документи та електронний документообіг». Структура Закону. Основні статті Закону. Мета Закону. Особливості застосування цього закону.

Тема 3. Основні стандарти ІБ. Основні стандарти з технології ІБ.

ДСТУ 3396.0-96. Мета стандарту. Структура стандарту. Вимоги стандарту. Основні положення стандарту. Особливості застосування.

ДСТУ 3396.1-96. Мета стандарту. Структура стандарту. Вимоги стандарту. Основні положення стандарту. Особливості застосування.

ДСТУ 4145-2002. Мета стандарту. Структура стандарту. Вимоги стандарту. Основні положення стандарту. Особливості застосування.

ДСТУ ГОСТ 28147-2009. Мета стандарту. Структура стандарту. Вимоги стандарту. Основні положення стандарту. Особливості застосування.

ДСТУ 3918.0-1999(ISO/IEC 1207-1995). Мета стандарту. Структура стандарту. Вимоги стандарту. Основні положення стандарту. Особливості застосування.

ДСТУ ISO/IEC TR 13335-1-2003. Мета стандарту. Структура стандарту. Вимоги стандарту. Основні положення стандарту. Особливості застосування.

ДСТУ ISO/IEC TR 13335-2-2003. Мета стандарту. Структура стандарту. Вимоги стандарту. Основні положення стандарту. Особливості застосування.

ДСТУ ISO/IEC TR 13335-3-2003. Мета стандарту. Структура стандарту. Вимоги стандарту. Основні положення стандарту. Особливості застосування.

ДСТУ ISO/IEC TR 13335-4-2005. Мета стандарту. Структура стандарту. Вимоги стандарту. Основні положення стандарту. Особливості застосування.

ДСТУ ISO/IEC TR 13335-5-2005. Мета стандарту. Структура стандарту. Вимоги стандарту. Основні положення стандарту. Особливості застосування.

Змістовий модуль 2. Створення КСЗІ в інформаційно-телекомунікаційних системах

Тема 1. Формування загальних вимог до КСЗІ в ІКС.

Призначення КСЗІ. Суб'єкти та об'єкти КСЗІ. Послідовність робіт зі створення КСЗІ.

Порядок проведення обстеження середовищ функціонування ІТС. Порядок оформлення моделі загроз, моделі порушника. Формування завдання на створення КСЗІ. Порядок розроблення, впровадження, експертні випробування, супроводження КСЗІ від несанкціонованих дій в ІС, ТС, ІКС.

Служба захисту інформації (СЗІ). Порядок створення, призначення та структура СЗІ. Завдання та функції СЗІ. Порядок організації робіт СЗІ.

Тема 2. Етапи побудови КСЗІ.

Порядок розробки політики безпеки (ПБ) інформації в ІКС. Основні положення ПБ в КСЗІ. Порядок документального оформлення ПБ. Розробка технічного завдання (ТЗ) на створення КСЗІ. Загальні вимоги та порядок розробки ТЗ на КСЗІ в АС. Вимоги до змісту розділів ТЗ. Порядок оформлення ТЗ. Порядок розробки проекту КСЗІ. Ескізний проект КСЗІ. Технічний проект КСЗІ. Робочий проект КСЗІ. Загальні вимоги до порядку введення КСЗІ в дію. Підготовка КСЗІ до введення в дію. Порядок проведення попередніх випробувань. Порядок проведення дослідної експлуатації. Основні положення проведення Державної експертизи КСЗІ. Порядок організації та проведення Державної експертизи КСЗІ.

Тема 3. Система управління інформаційною безпекою підприємства

Стандарти управління інформаційною безпекою (СУІБ). Методика формування нормативних, розпорядчих та методичних документів в процесі впровадження та функціонування СУІБ. Організаційна структура служби інформаційної безпеки. Варіанти оброблення ризиків. Вибір методу оброблення ризиків. Програмна підтримка аналізу ризиків. Оцінка відповідності СУІБ своєму призначенню відповідно до вимог діючих стандартів та нормативних документів.

2. Мета та цілі курсу -

Мета дисципліни «Стандартизація, сертифікація засобів та комплексів захисту інформації» є ознайомлення студентів із структурою законодавства Україні в області ІБ, основним законами в цій сфері, навчання студентів принципам побудови комплексних систем захисту інформації на основі синтезу організаційних і технічних заходів щодо забезпечення захисту інформації з обмеженим доступом, основ ведення електронного документообігу в умовах сучасних кіберзагроз та витоку технічними каналами, забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації.

Основними завданнями вивчення дисципліни є опанування теоретичними знаннями та набуття практичних навичок з питань стандартизації, сертифікації засобів та комплексів захисту інформації, застосування нормативної документації щодо ліцензування, стандартизації й сертифікації комплексів захисту інформації в Україні на практиці.

Програмні компетентності:

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації

КФ 1. Здатність розробляти та впроваджувати законодавчу, нормативно-правову базу, державні і міжнародні вимоги, а також інтегрувати, аналізувати і використовувати сучасні світові практики та стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки

КФ 4. Здатність розробляти, впроваджувати та аналізувати заходи, щодо резервування інформаційних ресурсів, розробки планів відновлення штатного функціонування інфраструктури організації в цілому, які викликані реалізацією різного класу кібератак, виявленням і реєстрацією інцидентів та нештатних ситуацій.

3. Результати навчання –

У результаті вивчення навчальної дисципліни студент повинен:

Знати**:**

- теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах;
- нормативно-правові документи у сфері захисту інформації, зокрема, щодо створення КСЗІ;
- основні поняття із стандартизації та сертифікації;
- нормативно-правову документацію із стандартизації та технічного захисту інформації;
- порядок розроблення, прийняття, перевірки, внесення змін та перегляду стандартів;

– правила, схеми та порядок проведення робіт із сертифікації засобів захисту інформації;
– ліцензійну діяльність в галузі технічного захисту інформації; порядок проведення акредитації;

Вміти:

- діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки;
- виконувати налаштування інформаційних систем та комунікаційного обладнання;
- виконувати захист інформаційних систем від комп'ютерних вірусів;
- забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил.
- оформляти документацію для подачі у відповідні органи стандартизації, сертифікації, ліцензування й акредитації.

ПРН

З - використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності

4 - аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності,які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

6- діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, в тому числі міжнародних в галузі інформаційної та/або кібербезпеки;

7- проектувати, впроваджувати, та супроводжувати інформаційно-комунікаційні системи, а також забезпечувати захист інформаційних ресурсів мереж (мережева безпека) та всієї інфраструктури установи на базі сучасних моделей, методів і засобів передачі даних в комутативних або без комутативних каналах зв'язку, хмарного простору, протоколів обміну даними, мережного устаткування, тощо ;

9- розробляти, впроваджувати та аналізувати заходи, щодо резервування інформаційних ресурсів, розробки планів відновлення штатного функціонування інфраструктури організації в цілому, які викликані реалізацією різного класу кібератак, виявленням і реєстрацією інцидентів та нештатних ситуацій.

4. Обсяг курсу. Зазначте загальку кількість кредитів, кількість занять та годин самостійної роботи

Вид заняття	**Загальна к-сть годин**
лекції	16
лабораторні	14
самостійна робота (РГР)	90

5. Пререквізити - Взаємозв'язок із суміжними дисциплінами: вивчення навчальної дисципліни "Стандартизація, сертифікація засобів та комплексів захисту інформації" поглиблює знання студентів отримані під час вивчення таких дисциплін "Основи криптографічного захисту інформації", "Інформаційна безпека держави", "Забезпечення інформаційної безпеки" й "Основи національної безпеки", «Основи технічного захисту інформації», «Програмний захист інформації», «Менеджмент інформаційної безпеки», «Безпека в інформаційно-комунікаційних системах» (при підготовці фахівців освітньо-кваліфікаційного рівня "бакалавр" за напрямом "Кібербезпека)". Дисципліна "Комплексні системи захисту інформації" дає фундаментальні знання для вивчення пропонованої дисципліни.

6. Система оцінювання та вимоги

Оцінювання проводиться за 100-бальною шкалою.

Бали нараховуються за наступним співвідношенням:

• лабораторні роботи : 20% семестрової оцінки;

• домашні завдання: 20% семестрової оцінки;

•РГР: 20% семестрової оцінки;

• іспит: 40% семестрової оцінки.

7. Політики курсу -

Політика щодо академічної доброчесності: Списування під час контрольних робіт заборонені (в т.ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки лабораторних завдань.

Жодні форми порушення академічної доброчесності не толеруються. У випадку таких подій – реагування відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників Чернігівського національного технологічного університету та Методичних рекомендацій для закладів вищої освіти з підтримки принципів академічної доброчесності

Правила перезарахування кредитів у випадку мобільності, правила перескладання або відпрацювання пропущених занять тощо: відбувається згідно з Положення про організацію освітнього процесу в ЧНТУ.

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності балів).

Перескладання модулів відбувається за наявності поважних причин (наприклад, лікарняний).

Політика щодо відвідування: Відвідування занять є обов’язковим компонентом оцінювання. За об’єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням.

8. Рекомендована література

Базова

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994);
2. Закон України “Про захист персональних даних” (2010)
3. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)
4. Закон України “Про національну безпеку (2018)
5. Стратегія кібербезпеки України” (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)
6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229;
7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;
8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;
9. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
10. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ, К: 1999. – 34с.
11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
12. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.
13. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
14. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.
15. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
16. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
17. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
18. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.
19. НД ТЗІ 1.6-004-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.
20. 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

Допоміжна

1. Основи стандартизації: підручник / О.В. Заболотний, М.Д. Кошовий, В.О. Книш та ін. – Х.: Нац. аерокосм. ун-т „Харк. авіац. Ін-т”, 2010.- 304 с.

2. Управління якістю. Сертифікація / [Бичківський Р.В., Столярчук П.Г., Сопільник Л.І., Калинський О.О.]. – К.: Вища школа, 2005. – 432 с.

4. Шаповал М.І. Менеджмент якості: Підручник.- К.: Т-во „Знання”, КОО, 2003.- 475 с.

3. Національні стандарти України: ДСТУ 1.1. – 1.7., 1.11., 1.12.

4. Національні стандарти України: ДСТУ 3396.0, ДСТУ 3396.1, ДСТУ 3396.2.

5. Журнали «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», «Стандартизація, сертифікація, якість», «Стандарты и качество», тощо.

Інформаційні ресурси

1. http://bezopasnost.biz
2. http://dstszi.gov.ua