СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Проектування технічних систем захисту інформації
Мова викладання	українська
Викладач	Петренко Тарас Анатолійович, доцент
Профайл викладача	Сайт кафедри: https://mmi.stu.cn.ua/personal-kafedry/ Google академія: https://scholar.google.com/citations?user=2bJE-4IAAAAJ&hl=ru
Контакти викладача	тел.: 0636419136, e-mail: mail_taras@ukr.net

1. Анотація курсу. Сьогодні забезпечення технічного захисту інформації є комплексною проблемою, вирішення якої потребує необхідної фахової підготовки, нормативного та методичного супроводження, технічного оснащення відповідних робіт. Безумовно, фахівець який не тільки в змозі організувати систему технічного захисту інформації за допомогою наявних технічних засобів, але і вміє проектувати та створювати нові технічні системи захисту інформації буде більш конкурентоспроможним на ринку праці.

На заняттях курсу «Проектування технічних систем захисту інформації» студенти отримують теоретичні знання та практичні вміння в сфері проектування, впровадження та професійної експлуатації технічних систем захисту інформації відповідно до поставлених задач. Знайомляться з теоретичними та прикладними аспектами проектування технічних систем захисту інформації. Розглядають методологічні підходи до проектування технічних систем захисту інформації. Проводять наукові дослідження в зазначених напрямках.

Успішне засвоєння дисципліни дозволяє магістру зі спеціальності 125 – Кібербезпека розширити коло застосування набутих раніше знань та практичних навичок для вирішення професійних задач організації захисту інформації, до якого традиційно включають і задачі технічного захисту інформації.

В результаті вивчення курсу студенти готують курсовий проект в якому проектують реальні технічні засоби та системи захисту інформації.

2. Мета та цілі курсу - формування науково-професійного світогляду магістра спеціальності 125 – Кібербезпека в області технічного захисту інформації шляхом дослідження та ґрунтовного засвоєння основ проектування, створення та забезпечення функціонування технічних систем захисту інформації в інформаційно-телекомунікаційних системах підприємств, установ та організацій а також принципів організації охорони спеціальних об’єктів.

Об’єкт – системи технічного захисту інформації

Предмет – сучасні методи проектування технічних систем захисту інформації; основні теоретичних положення створення ТСЗІ; процеси проектування систем захисту інформації, тобто виконання проектних робіт, що включає в себе розробку технічної документації ТСЗІ, її технічну підтримку та супровід, погодження у відповідних державних і відомчих органах, особливості проектування ТСЗІ відповідно до чинних вимог нормативних документів із дотриманням правил інформаційної безпеки.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програ-

мою спеціальності 125 - Кібербезпека:

КЗ1.Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Знання та розуміння предметної області та розуміння професії.

КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ5.Здатність до пошуку,оброблення та аналізу інформації з різних джерел.

КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (автоматизованих систем та їх додатків) та у інфраструктурі організації в цілому.

КФ 8. Здатність проводити науково-освітню діяльність, розробляти та впроваджувати систему управління персоналом, а також проводити та планувати навчання працівників компанії і наукові дослідження в галузі інформаційних технологій у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації у відповідність вітчизняним та світовим стандартам галузі інформаційної та/або кібербезпеки.

Основними завданнями вивчення дисципліни “Проектування технічних засобів захисту інформації” є:

– ознайомлення з сучасним станом та тенденціями розвитку проблеми проектування ТЗЗІ;

– вивчення різновидів ТЗЗІ;

– засвоєння принципів застосування цих закономірностей для проектування ТЗЗІ;

– практичне ознайомлення з особливостями та засвоєння основ робіт з проектування СТЗІ та ТЗЗІ.

3. Результати навчання:

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН 1. постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

ПРН 2. планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН 3. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 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;

ПРН 5. реалізовувати процеси постійної самоосвіти і професійної сертифікації, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН 8. проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту додатків (веб - додатків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації;

ПРН14. розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності, згідно встановленої політики інфо-

рмаційної безпеки та/або кібербезпеки і стратегії організації.

У підсумку ЗВО повинні ***знати :***

- базові терміни та визначення в галузі технічного захисту інформації;
- українські та міжнародні стандарти систем технічного захисту інформації;
- основі технічні канали витоку інформації;
- способи несанкціонованого перехоплення інформації;
- особливості роботи з засобами технічного захисту інформації;
- тенденції розвитку систем технічного захисту інформації;
- основні технічні системи, що використовуються для несанкціонованого перехоплення інформації;
- основні технічні системи, що використовуються для захисту інформації від несанкціонованого перехоплення;
- основи методів проектування ТСЗІ;
- порядок проектування ТЗЗІ та ТСЗІ.
- основні положення політики безпеки об'єктів, принципи, за якими категоруються об'єкти, різновиди засобів виявлення порушників та технічних каналів витоку інформації, а також організацію контролю доступу на об'єкт, та ін.

вміти :

- проектувати ТЗЗІ та ТСЗІ та їх елементи з урахуванням усіх аспектів поставленої задачі, включаючи створення, налагодження, експлуатацію та технічне обслуговування;
- проектувати, встановлювати, налаштовувати та обслуговувати системи відеонагляду, протипожежні системи та сигналізації;
- експлуатувати прилади та системи виявлення закладних пристроїв негласного зйому інформації;
- забезпечувати надійний захист інформації за допомогою ТСЗІ від її витоку по технічним каналам;
- застосовувати отримані знання під час виконання курсового проекту з дисципліни, що вивчається, у дипломному проектуванні а також у майбутній професійній діяльності.

4. Обсяг курсу. 3 кредитів ECTS, що становить 90 годин роботи студентів, з них 130 годин самостійної роботи та 50 годин аудиторної роботи з викладачем.

Вид заняття	**Загальна кількість годин**
Лекції	26
Лабораторні заняття	24
Самостійна робота (РГР, наукові дослідження)	130

Тематика курсу

Змістовий модуль 1. Прикладні аспекти проектування технічних систем захисту інформації

Тема 1. Технічні канали витоку інформації

Тема 2. Фізичні основи захисту інформації від витоку по технічним каналам

Тема 3. Технічні системи захисту від витоку інформації по технічним каналам

Тема 4. Технічні засоби пошуку та виявлення закладних пристроїв

Тема 5. Технічні системи контролю доступу до приміщень

Тема 6. Технічні системи протипожежних систем

Тема 7. Технічні системи спостереження

Тема 8. Технічні системи сигналізацій та систем охорони периметру

Змістовий модуль 2. Методологічні підходи до проектування технічних систем захисту інформації

Тема 9. Аналіз інформаційного процесу як середовища захисту інформації

Тема 10. Моделювання систем захисту інформації

Тема 11. Методи проектування технічних системи захисту інформації

Тема 12. Розробка проекту технічної системи захисту інформації

Тема 13. Впровадження, визначення якості і управління технічними системами захисту інформації

5. Пререквізити. Передумовою для вивчення курсу «Проектування технічних систем захисту інформації» є успішне засвоєння дисциплін: фізика, інформатика, архітектура комп'ютерних систем, комп'ютерна схемотехніка, та ін. Дисципліна «Проектування технічних систем захисту інформації» є базовою для подальшої успішної професійної діяльності за спеціальністю, а також може використовуватися під час підготовки випускної кваліфікаційної роботи магістра.

6. Система оцінювання та вимоги

Загальна система оцінювання курсу	ECTS
Вимоги до курсового проекту	Курсовий проект, який відповідає викладеним у методичних рекомендаціях вимогам, оцінюється за стобальною шкалою з урахуванням якості виконаної роботи, виступу студента і його відповідей на запитання членів комісії по захисту. Слід пам'ятати, що висока якість виконаного курсового проекту не є гарантією її високої оцінки, оскільки оцінка може бути зниженою через некваліфікований захист курсової роботи. При перевірці та оцінюванні курсового проекту враховується повнота розкриття теми, актуальність та практична значимість, самостійність виконання, вчасність здачі роботи та відповідність оформлення результатів діючим вимогам
Лабораторні заняття	Кожна виконана лабораторна робота оцінюється від 0 до 3-х балів. Кількість балів залежить від рівня теоретичних знань та практичних навичок студента за темою, самостійності виконання роботи та вчасності її захисту
Умови допуску до підсумкового контролю	Умовою допуску до екзамену є виконання та отримання хоча б мінімальної кількості балів з усіх обов'язкових видів навчальної роботи передбачених робочою програмою (лабораторних, модульного контролю та РГР). Мінімальна кількість балів необхідна для допуску до екзамену – 20.

Модуль за тематичним планом дисципліни та форма контролю	**Кількість балів**
Змістовий модуль 1. Прикладні аспекти проектування технічних засобів захисту	

Модуль за тематичним планом дисципліни та форма контролю		Кількість балів	
інформації			
1	Повнота ведення конспектів занять (присутність на лекції+конспект – 1 бал за кожну лекцію)	0	8
2	Підготовленість до лабораторних робіт. Рівень знань студента за темою лабораторної роботи (максимум - 2 бали за кожну лаб. роботу)	0	12
3	Самостійність виконання лабораторних робіт (максимум 0,5 бала)	0	6
4	Своєчасність виконання лабораторних робіт (максимум 0,5 бала)	0	6
5	Самостійна робота	0	8
6	Поточний модульний контроль	0	5
Змістовий модуль 2. Методологічні підходи до проектування технічних засобів захисту інформації			
1	Повнота ведення конспектів занять (присутність на лекції+конспект – 1 бал за кожну лекцію)	0	5
2	Самостійна робота	0	5
3	Поточний модульний контроль	0	5
Семестрова оцінка поточного контролю		**0**	**60**
Екзамен		**0**	**40**
Всього		**0**	**100**

Шкала оцінювання: національна та ECTS

Критерії оцінювання	Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
			для екзамену, КП	для заліку
Студент виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили, проводить наукові дослідження	90 – 100	**A**	відмінно	зараховано
Студент вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв’язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна	82-89	**B**	добре	
Студент вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттє-	75-81	**C**		

Критерії оцінювання	Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
			для екзамену, КП	для заліку
ві, добирати аргументи для підтвердження думок				
Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих	66-74	**D**	задовільно	
Студент володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні	60-65	**E**		
Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу	0-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання

7. Політики курсу.

7.1 Академічна доброчесність – самостійність виконання навчальних завдань та посилання на джерела у випадку використання напрацювань інших авторів. Види порушень академічної доброчесності – академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво.

Відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників Національного університету «Чернігівська політехніка» Затв. Вченою радою НУ «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 Введено в дію наказом ректора від 31 серпня 2020 р. № 26 за порушення академічної доброчесності здобувачі освіти можуть мати наслідком: повторне проходження оцінювання (контрольна робота, іспит, залік тощо); повторне проходження відповідного освітнього компонента освітньої програми; відрахування із закладу освіти (крім осіб, які здобувають загальну середню освіту); позбавлення академічної стипендії; позбавлення наданих закладом освіти пільг з оплати навчання.

7.2 Політика дедлайнів – своєчасність здачі лабораторної роботи оцінюється в 0,5 бала за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 2 бали. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом).

7.3 Політика перезарахування кредитів у випадку мобільності – перезарахування відбувається якщо назви навчальних дисциплін ідентичні або мають незначну стилістичну відмінність, але обсяги та змістова частина навчальних програм не відрізняються; кількість кредитів, відведена на вивчення навчальної дисципліни відрізняється менше, ніж на 25 %; форми підсумкового контролю з дисциплін однакові. При перезарахуванні дисципліни зберігається раніше здобута позитивна оцінка. Перескладання іспиту з

дисципліни з метою підвищення оцінки, визначеної в документах виданих здобувачу вищої освіти за попереднім місцем навчання, не дозволяється. Перезарахування кредитів проводиться відповідно до Порядку визначення академічної різниці та перезарахування навчальних дисциплін у Національному університеті «Чернігівська політехніка» Затв. Вченою радою НУ «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 Введено в дію наказом ректора від 31 серпня 2020 р. № 26.

7.4 Політика щодо відвідування – відвідування занять є обов'язковим. При наявності поважних причин (хвороба, участь в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом) студенти можуть узгодити з викладачем індивідуальний графік навчання та здачі всіх видів навчальної роботи. Студенти можуть перескладати або відпрацьовувати пропущені заняття на консультаціях викладача чи у спеціально відведений викладачем для цього час.

7.5 Політика щодо правил поведінки на заняттях – активна участь у навчальному процесі, виконання необхідного мінімуму навчальної роботи, коректна поведінка щодо інших учасників навчального процесу, взаємоповага, використання мобільних пристроїв тільки для навчання.

7.6 Політика заохочень та стягнень. Результати навчальної, наукової та організаційної діяльності студентів за напрямами курсу їм можуть нараховуватися додаткові бали - до 10 балів, в залежності від вагомості досягнень студента. Види позанавчальної діяльності, за які студенти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, статті на науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

8. Рекомендована література та інформаційні джерела

1. Information Technology Security Evaluation Criteria, v. 1.2. – Office for Official publications of the European Communities, 1991 [Electronic resource]. – Access mode : www.fbi.gov.
2. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006.
3. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации / Г.А. Бузов. – М.: Горячая линия – Телеком, 2010. – 240 с.
4. Гайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Гайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.
5. Державна служба спеціального зв'язку та захисту інформації України. – [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua
6. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
7. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
8. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2007. – 382 с.
9. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.
10. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 510 с.

11. Рибальський О.В. Захист інформації в інформаційно-комунікаційних системах. Навчальний посібник для курсантів ВНЗ МВС України / О.В. Рибальський, В.Г. Хахановський, В.А. Кудінов, В.М. Смаглюк. – К.: Вид. Національної академії внутріш. справ, 2013. – 118 с.

12. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

13. Хорошко В. А. Методы и средства зашиты информации / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с.