СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**Ступінь освіти**	бакалавр
	Галузь знань	12 Інформаційні технології
	Тривалість викладання	11,12 чверті
	Заняття:	Весінній семестр
	лекції:	2 години
	практичні заняття:	1 година
	Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»:
https://do.nmu.org.ua/enrol/index.php?id=5809

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладачів

Ткач Максим Олександрович	к.т.н., доцент
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/tkach.php
E-mail:	tkach.m.ol@nmu.one

1. Анотація до курсу

Дисципліна спрямована на підвищення рівня обізнаності щодо нормативно-правової бази у сфері ТЗІ та технічних засобів захисту інформації. У курсі викладені основні положення та нормативні акти для ТЗІ, канали витоку інформації, фізичні та апаратні засоби захисту інформації.

2. Мета та завдання курсу

Мета дисципліни – формування у студентів компетентності щодо видів, джерел та носіїв інформації, що підлягає захисту, технічних каналів витоку інформації, методів та засобів технічного захисту інформації, захисту інформації в каналах зв'язку, етапів побудови комплексів технічного захисту інформації, контролю ефективності технічного захисту інформації.

Завдання курсу:

− надання студентам теоретичних знань про системи технічного захисту інформації;
− формування у студентів категоріальних понять з використання СТЗІ;
− формування у студентів уміння аналізу каналів витоку;

− стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів застосування систем технічного захисту інформації та набуття наступних фахових компетентностей:

3. Результати навчання

Володіти принципами, техніками та засобами розробки або дослідження, що використовуються у предметній області розробки або дослідження; створювати прототипи програмного забезпечення, щоб переконати-ся, що воно відповідає вимогам до розробки; виконувати його тестування і статичний аналіз, щоб переконатися у відповідності завданню розробки або дослідження.

Знати:

– історію та особливості розвитку СТЗІ;

– основні процеси що вимагаються при використанні засобів ТЗІ;

– класифікацію та характеристики апаратних засобів для ефективного їх впровадження;

– основні чинники, що визначають надійність і ефективність СТЗІ;

– понятійно-термінологічний апарат в області застосування СТЗІ;

Вміти:

– визначати тип каналів витоку;

– аналізувати ефективність обраного засобу технічного захисту,

– виявляти особливості технічного забезпечення для різних типів задач;

– обґрунтовувати вибір технічних засобів для ефективного впровадження засобів ТЗІ;

– визначати ресурси, необхідні для забезпечення надійності функціонування СТЗІ з врахуванням факторів помилки користувачів;

4. Структура курсу

ЛЕКЦІЇ

Змістовний модуль №1

1. Види, джерела та носії інформації, що підлягає захисту

1.1. Технічний захист інформації. Види інформації, що підлягає технічному захисту.

1.2. Джерела та носії інформації, що захищається технічними засобами.

1.3. Створення комплексів технічного захисту інформації. Основні етапи. Нормативна база.

2. Технічні канали витоку інформації, що обробляється ТЗПІ

2.1 Структура та класифікація технічних каналів витоку інформації.

2.2 Фізична природа електромагнітних каналів витоку інформації, що обробляється ТЗПІ. Методи та засоби захисту інформації від витоку електромагнітними каналами

2.3 Фізична природа електричних каналів витоку інформації, що обробляється ТЗПІ. Методи та засоби захисту інформації від витоку електричними каналами.

2.4 Фізична природа параметричного каналу витоку інформації, що обробляється ТЗПІ. Методи та засоби захисту інформації від витоку параметричним каналом.

2.5 Методи та засоби захисту інформації від витоку при передачі телефонними лініями зв’язку

Змістовний модуль №2

3. Акустичні та віброакустичні технічні канали витоку інформації

3.1 Фізичні основи акустичних та віброакустичних сигналів

3.2 Технічні засоби розвідки акустичної та віброакустичної інформації

3.3 Методи та засоби захисту акустичної та віброакустичної інформації від витоку технічними каналами.

3.4 Методи та засоби виявлення та локалізації закладних пристроїв

4 Методики та засоби оцінки ефективності захисту інформації від витоку технічними каналами

4.1. Загальні вимоги до методик оцінки ефективності захисту інформації від витоку технічними каналами

4.2. Методики та засоби оцінки рівня захищеності інформації від витоку за рахунок ПЕМВ

4.3. Методики та засоби оцінки рівня захищеності інформації від витоку провідними лініями

4.4. Методики та засоби оцінки рівня захищеності інформації від витоку акустичними та віброакустичними каналами

ПРАКТИЧНІ ЗАНЯТТЯ

1. Дослідження технічних каналів витоку інформації та засобів захисту

1.1 Дослідження акустоелектричного каналу витоку інформації

1.2 Дослідження мережевих протизавадних фільтрів.

1.3 Дослідження видів екранування. Оцінка ефективності екранування

1.4 Засоби захисту інформації від витоку при передачі провідними телефонними лініями зв’язку

2 Пошук та локалізація закладних пристроїв

2.1 Пошук та локалізація закладних пристроїв детекторами поля

2.2 Пошук та локалізація закладних пристроїв нелінійним локатором

2.3 Пошук та локалізація закладних пристроїв комплексом «Пиранья»

2.4 Пошук та локалізація закладних пристроїв комплексом «Акор-2ПК»

3 Методики та засоби оцінки ефективності захисту інформації від витоку технічними каналами

3.1 Оцінка рівня звукоізоляції та віброізоляції комплексом «Пиранья»

3.2 Оцінка рівня захищеності інформації від витоку за рахунок ПЕМВ комплексом «Акор-2ПК»

3.3 Оцінка рівня захищеності інформації від витоку провідними лініями комплексом «Пиранья

3.4 Оцінка рівня захищеності інформації від витоку провідними лініями комплексом «Акор-2ПК»

5. Технічне обладнання та/або програмне забезпечення

Система дистанційного навчання НТУ ДП Детектори поля „RD-14” та „PROTECT-1203”. Нелінійний локатор «NR-m».

Тестовий інфрочервоний передавач „IRT-700”. Тестовий радіопередавач „TTM-700”.

Багатофункціональний пошуковий пристрій ST-031P „ПІРАНЬЯ”. Автоматизований комплекс радіомоніторингу та пошуку закладних пристроїв, виявлення і вимірювання ПЕМВН від засобів ЕОТ "АКОР-2ПК".

Лабораторні стенди.

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	45	30	0	**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.

15 балів – Достатня зрозумілість відповіді

10 бали – Добра зрозумілість відповіді

7 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.

8 Рекомендовані джерела інформації

8.1. Основні

1. Закон України "Про інформацію".
2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
3. Закон України "Про основи національної безпеки".
4. Постанова Кабінету Міністрів України від 27.11.1998 № 1893 «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію».
5. Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.
6. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.
7. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
8. ДСТУ 33962-97 Захист інформації. Технічний захист інформації. Терміни та визначення;
9. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
10. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
11. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
12. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
13. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
14. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.
15. 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.
16. 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.

8.2. Допоміжні

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко, 2015. – 449 с.
2. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. –К.: "МК-Прес", 2005. – 432 с.
3. Хорошко В.О, Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки : К.: ДУІКТ, 2008. – 186 с.

8.2. Додаткові ресурси

1. Державна служба спеціального зв’язку та захисту інформації – Режим доступу: dsszzi.gov.ua
2. Офіційний портал Верховної ради України – Режим доступу: rada.gov.ua
3. Технічний захист інформації – Режим доступу: tzi.ua/ua/tz.htm