МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Кафедра захисту інформації

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Проектування, впровадження та супровід комплексних систем захисту інформації

Освітня програма: Безпека інформаційних і комунікаційних систем

Спеціальність: 125 Кібербезпека

Галузь знань: 12 Інформаційні технології

Ступінь вищої освіти: Перший (бакалаврський) рівень

Затверджено на засіданні кафедри
захисту інформації
Протокол №____ від _____ р.

м. Запоріжжя 2020

1. Загальна інформація	
Назва дисципліни	*ППН 11. Проектування, впровадження та супровід комплексних систем захисту інформації, обов'язкова.*
Рівень вищої освіти	*Перший (бакалаврський) рівень*
Викладач	*Лізунов Сергій Іванович, к.т.н., доцент, доцент.*
Контактна інформація викладача	*Телефон кафедри 7698491, викладача 7698597, s.i.lizunov@i.ua*
Час і місце проведення навчальної дисципліни	*Згідно розкладу занять викладачів кафедри.* https://zp.edu.ua/kafedra-zahistu-informaciyi
Обсяг дисципліни	*7,5 кредитів ЄКТС, 225 годин.* *Розподіл годин:* *- 5,5 кредитів ЄКТС, 165 годин теоретичні та практичні заняття, лекції 52 години, практичні 52 години, самостійна робота 61 година.* *– 2 кредити ЄКТС, 60 годин курсовий проєкт.* *Семестр вивчення навчальної дисципліни: 7 і 8 семестри.* *Вид контролю: залік в кінці 7 і 8 семестру, захист курсової роботи в кінці 8 семестру.*
Консультації	*Згідно з графіком консультацій.* https://zp.edu.ua/kafedra-zahistu-informaciyi

2. Пререквізити і постреквізити навчальної дисципліни

Пререквізити: Нормативно-правове і організаційне забезпечення інформаційної безпеки. Основи теорії кіл, сигналів та процесів в електроніці. Телекомунікаційні та комп'ютерні мережі. Захист інформації в банківській сфері та електронному бізнесі. Менеджмент інформаційної безпеки. Антивірусні технології. Захист програмного забезпечення. Методи та засоби технічного захисту інформації. Захищені мережні технології.

Компетентності:

КЗ 1. Здатність застосовувати знання в практичних ситуаціях.

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

Постреквізіти: Переддипломна практика. Дипломування.

3. Характеристика навчальної дисципліни

Дисципліна «Проектування, впровадження та супровід комплексних систем захисту інформації» є базовою у підготовці фахівця з інформаційної безпеки.

Перелік загальних и фахових компетентностей, яких набуває студент при вивченні:

КЗ 1. Здатність застосовувати знання в практичних ситуаціях.

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

КЗ 4 Вміти виявляти, ставити та вирішувати проблеми за професійним спрямуванням, здійснювати професійну діяльність на основі техніко-економічного аналізу.

КЗ 5 Здатність до пошуку, оброблення та аналізу інформації.

КФ 1. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах

КФ 3. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.

КФ 4. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах

КФ 7. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

Програмні результати навчання:

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

ПРН 4. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 5. 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 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності, що базуються на культурно-історичних, світоглядних та державницьких аспектах.
ПРН 8. Використовувати знання про фізичні явища та володіти математичним апаратом для моделювання об'єктів інформаційної діяльності
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 28. Виявляти небезпечні сигнали технічних засобів.

4. Мета вивчення навчальної дисципліни

Формування у студентів навиків проєктування, впровадження та супроводу комплексних систем захисту інформації.

5. Завдання вивчення дисципліни

Основне завдання навчальної дисципліни – формування у студентів системних знань і компетентностей з проєктування, впровадження та супроводу комплексних систем захисту інформації.

6. Зміст навчальної дисципліни

Перший семестр. Модуль 1.
Змістовий модуль 1.

Тема 1 Основні положення політики безпеки підприємства – основа для проектування системи захисту інформації.
Тема 2. Моделі порушників.
Тема 3. Основні етапи проектування систем охорони і захисту інформації.
Тема 4. Спеціальні методи захисту за допомогою спеціальної апаратури та проведення моніторингу.

Змістовий модуль 2.

Тема 5. .Датчики і їх різновиди. Застосування датчиків у системах охорони спеціальних об'єктів.
Тема 6. Радіохвильові і радіопроменеві засоби виявлення порушників.
Тема 7. Застосування оптичних засобів виявлення порушників.

Другий семестр. Модуль 2.
Змістовий модуль 3.

Тема 8. Системи охорони периметру об'єктів.
Тема 9. Магнітометричні засоби виявлення металевих предметів.
Тема 10. Охоронне телебачення та відеоспостереження.

Змістовий модуль 4.

Тема 11. Контроль доступу.
Тема 12. Захист телефонних ліній.
Тема 13. Лінії передавання у системах захисту інформації.
Тема 14. Апаратура захисту інформації.

7. План вивчення навчальної дисципліни

№ тижня	Назва теми Форми організації навчання		Кількість годин
	Перший семестр		
1,2	*Тема 1. Основні положення політики безпеки підприємства – основа для проектування системи захисту інформації.*	лк	4
	Системний підхід при формуванні системи захисту інформації.	пр	4
3,4	*Тема 2. Моделі порушників.*	лк	4
	Інформаційна безпека та кадрова політика на підприємстві.	пр	4

5,6	*Тема 3. Основні етапи проектування систем охорони і захисту інформації.*	лк	4
	Освоєння методики проведення розрахунків для систем захисту об'єктів інформатизації	пр	4
7,8	*Тема 4. Спеціальні методи захисту за допомогою спеціальної апаратури та проведення моніторингу.*	лк	4
	Канали витоку інформації в будівлі, службових приміщеннях і інженерних системах будівлі.	пр	4
Рубіжний контроль.			
9-11	*Тема 5. .Датчики і їх різновиди. Застосування датчиків у системах охорони спеціальних об'єктів.*	лк	6
	Вивчення принципів дії та галузей застосування сучасних датчиків.	пр	6
12,13	*Тема 6. Радіохвильові і радіопроменеві засоби виявлення порушників*	лк	4
	Засоби радіотехнічної і радіорозвідки, їх характеристики.	пр	4
14,15	*Тема 7. Застосування оптичних засобів виявлення порушників.*	лк	4
	Виток інформації по оптичним каналам.	пр	4
Рубіжний контроль. Підсумковий семестровий контроль - залік.			
Другий семестр			
1,2	*Тема 8. Системи охорони периметру об'єктів.*	лк	4
	Системи просторового зашумлення об'єктів ЕОТ.	пр	4
3,4	*Тема 9. Магнітометричні засоби виявлення металевих предметів.*	лк	4
	Металошукачі та локатори нелінійностей.	пр	4
5,6	*Тема 10. Охоронне телебачення та відеоспостереження.*	лк	4
	Канали витоку інформації - робочі місця користувачів і персоналу.	пр	4
Рубіжний контроль.			
7,8	*Тема 11. Контроль доступу.*	лк	4
	Канали витоку інформації - структурована кабельна система.	пр	4
9	*Тема 12. Захист телефонних ліній.*	лк	2
	Засоби і способи перехоплення акустичних сигналів.	пр	2
10	*Тема 13. Лінії передавання у системах захисту інформації.*	лк	2
	Безпека оптоволоконних кабельних систем.	пр	2
11	*Тема 14. Апаратура захисту інформації.*	лк	2
	Способи захисту інформації при експлуатації слабкострумового обладнання.	пр	2
Рубіжний контроль. Підсумковий семестровий контроль - залік.			

8. **Самостійна робота**

Самостійна робота включає в себе: вивчення теоретичного матеріалу, підготовку до практичних робіт, виконання курсового проєкту, підготовку до рубіжного та підсумкового контролю.

8.1 Курсовий проєкт

Мета курсового проєкту є закріплення у студентів загальних положень, а також закріплення системного підходу щодо методів та засобів захисту інформації.

У якості завдання кожному студентові пропонується на підґрунті бази даних моделі об'єкта захисту розробити модель порушника й, на її основі, політику безпеки з вибором і обґрунтуванням технічних засобів захисту інформації.

Курсовий проєкт спрямований на формування практичних навичок проєктування комплексної системи захисту об'єктів.

У якості вихідних даних студенти вибирають об'єкт захисту у вигляді офісу фірми, виділеного приміщення, у якому здійснюється робота з конфіденційною інформацією, кімнати для переговорів і т.п.

Моделювання об'єктів захисту включає:

– структурування інформації, що захищається;

– розробку моделей об'єктів захисту.

Для структурування інформації як вихідних даних використовуються:

– перелік відомостей, що становлять державну, відомчу або комерційну таємницю;

– перелік джерел інформації в організації.

Структурування інформації проводиться шляхом класифікації інформації у відповідності зі структурою, функціями й завданнями організації із прив'язкою елементів інформації до її джерел. Деталізацію інформації доцільно проводити до рівня, на якім елементу інформації відповідає одне джерело.

Крім того, курсовий проєкт повинен містити в собі:

1. Докладний опис об'єкта захисту і видів інформації, що опрацьовується і зберігається на об'єкті,

2. Оцінку можливих каналів витоку інформації на об'єкті і їхній опис.

3. Перелік організаційних заходів на об'єкті.

4. Перелік організаційно-технічних заходів на об'єкті.

5. Перелік технічних заходів на об'єкті.

6. Розрахунок необхідних розмірів контрольованої зони і максимально припустимих відстаней розташування основних і допоміжних засобів на об'єкті.

7. Архітектуру системи захисту інформації на об'єкті і її схеми.

8. Оцінку очікуваної ефективності застосування системи захисту інформації на об'єкті.

При розробці пп, 3,4,5 і 6 необхідно звернути увагу на вирішення таких питань:

- захист основних і допоміжних технічних засобів об'єкта від перехоплення побічних електромагнітних випромінювань;

- захист систем заземлення об'єкта;

- захист систем електроживлення об'єкта;

- застосування просторового зашумлення і електромагнітного маскування об'єкта.

Склад, обсяг і терміни виконання змістових модулів курсової роботи дисципліни наведені у таблиці.

№ тижня	Назва теми	Кількість годин
1	*Ознайомлення із завданням, підбір і аналіз літератури*	*4*
2	*Структурування інформації, що захищається*	*4*
3	*Моделювання можливих каналів витоку інформації*	*6*
4	*Оцінка ступеня загрози інформації, що захищається*	*4*
5	*Розробка заходів щодо захисту інформації на даному об'єкті*	*6*
6	*Вибір технічних засобів захисту інформації на даному об'єкті*	*4*
7	*Розробка схеми розміщення технічних засобів на об'єкті*	*8*
8	*Оцінка ступеня захищеності інформації*	*4*
9	*Оптимізація проекту за вартістю захисту*	*4*
10,11	*Оформлення презентації і пояснювальної записки, захист курсового проєкту*	16
Усього годин		60

8.2 Самостійна робота з теорії та практиці дисципліни.			
№ тижня	**Назва теми**	**Кількість годин**	**Консультації, годин**
Перший семестр			
1-2	*Тема 1. Основні положення політики безпеки підприємства – основа для проектування системи захисту інформації.*	*1*	*0,5*
	Системний підхід при формуванні системи захисту інформації.	*2*	*0,5*
3-4	*Тема 2. Моделі порушників.*	*1*	*0,5*
	Інформаційна безпека та кадрова політика на підприємстві.	*2*	*0,5*
5-6	*Тема 3. Основні етапи проектування систем охорони і захисту інформації.*	*1*	*0,5*
	Освоєння методики проведення розрахунків для систем захисту об'єктів інформатизації	*2*	*0,5*
7-8	*Тема 4. Спеціальні методи захисту за допомогою спеціальної апаратури та проведення моніторингу.*	*1*	*0,5*
	Канали витоку інформації в будівлі, службових приміщеннях і інженерних системах будівлі.	*2*	*0,5*
Підготовка до рубіжного контролю. Рубіжний контроль.		*2*	*1*
9-11	*Тема 5. .Датчики і їх різновиди. Застосування датчиків у системах охорони спеціальних об'єктів.*	*1*	*0,5*
	Вивчення принципів дії та галузей застосування сучасних датчиків.	*2*	*0,5*
12-13	*Тема 6. Радіохвильові і радіопроменеві засоби виявлення порушників*	*1*	*0,5*
	Засоби радіотехнічної і радіорозвідки, їх характеристики.	*2*	*0,5*
14-15	*Тема 7. Застосування оптичних засобів виявлення порушників.*	*1*	*0,5*
	Виток інформації по оптичним каналам.	*2*	*0,5*
Підготовка до рубіжного контролюю. Рубіжний контроль.		*3*	*1*
Підсумковий семестровий контроль - залік.		*4*	*1*
Другий семестр			
1-2	*Тема 8. Системи охорони периметру об'єктів.*	*1*	*0,5*
	Системи просторового зашумлення об'єктів ЕОТ.	*2*	*0,5*
3-4	*Тема 9. Магнітометричні засоби виявлення металевих предметів.*	*1*	*0,5*
	Металошукачі та локатори нелінійностей.	*2*	*0,5*
5-6	*Тема 10. Охоронне телебачення та відеоспостереження.*	*1*	*0,5*
	Канали витоку інформації - робочі місця користувачів і персоналу.	*2*	*0,5*
Підготовка до рубіжного контролю. Рубіжний контроль.		*3*	*1*
7-8	*Тема 11. Контроль доступу.*	*1*	*0,5*
	Канали витоку інформації - структурована кабельна система.	*2*	*0,5*
9	*Тема 12. Захист телефонних ліній.*	*1*	*0,5*
	Засоби і способи перехоплення акустичних сигналів.	*2*	*0,5*
10	*Тема 13. Лінії передавання у системах захисту інформації.*	*1*	*0,5*
	Безпека оптоволоконних кабельних систем.	*2*	*0,5*
11	*Тема 14. Апаратура захисту інформації.*	*1*	*0,5*

	Способи захисту інформації при експлуатації слабкострумового обладнання.	*2*	*0,5*
Підготовка до рубіжного контролю. Рубіжний контроль.		*3*	*1*
Підсумковий семестровий контроль - залік.		*4*	*1*

9. Система та критерії оцінювання курсу

Поточний, рубіжний, семестровий контроль (з урахуванням відвідування занять, виконання практичних робіт, тестування при здачі модулів та заліку).

Форма проведення контролю: усна, письмова, комбінована, а також шляхом тестування з використанням програмно-технічних засобів.

9.1 Розподіл балів, які отримують студенти

Рубіжний контроль 1

Змістовий модуль №1			*Змістовий модуль № 2*		
Тема 1-Тема 4	*Практичні заняття №1-№4*	*Сума 1*	*Тема 5-Тема 7*	*Практичні заняття №5-7*	*Сума 2*
40	*60*	*100*	*40*	*60*	*100*

Підсумковий семестровий контроль

Бали за змістові модулі	*Сума*	*Бали за семестровий контроль*	*Сума*	*Залік*	*Сума*
0.4 (Сума 1+ Сума 2)	*80*		*20*		*100*

Рубіжний контроль 2

Змістовий модуль №3			*Змістовий модуль № 4*		
Тема 8 -Тема 10	*Практичні заняття №8-10*	*Сума 1*	*Тема 11-Тема 14*	*Практичні заняття №11-14*	*Сума 2*
40	*60*	*100*	*40*	*60*	*100*

Підсумковий семестровий контроль

Бали за змістові модулі	*Сума*	*Бали за семестровий контроль*	*Сума*	*Залік*	*Сума*
0.4 (Сума 1+ Сума 2)	*80*		*20*		*100*

9.2 Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	*Оцінка ECTS*	*Оцінка за національною шкалою*	
		для екзамену, курсового проекту (роботи), практики	*для заліку*
90 – 100	***A***	*відмінно*	*зараховано*
82-89	***B***	*добре*	
74-81	***C***		
64-73	***D***	*задовільно*	
60-63	***E***		
35-59	***FX***	*незадовільно з можливістю повторного складання*	*не зараховано з можливістю повторного складання*
0-34	***F***	*незадовільно з обов'язковим повторним вивченням дисципліни*	*не зараховано з обов'язковим повторним вивченням дисципліни*

10. Політика курсу

Викладач пояснює студентам систему організації навчального процесу та правил поведінки студентів на заняттях. Усі завдання, передбачені програмою, мають бути виконані у встановлені терміни. Успішність засвоєння навчального матеріалу визначається числом балів, отриманих при контрольних заходах. Максимальне число балів за змістовий модуль дорівнює 100: 40 балів за результатами тестування з теоретичного матеріалу, 60 балів за виконання 4 (3) практичних робіт. Кожна практична робота оцінюється 15 (20) балами: 5 балів за відповіді на контрольні питання до роботи, 10 (15) балів за виконання і захист роботи. Максимальне число балів підсумкового семестрового контролю дорівнює 100 і складаються: з суми балів змістових модулів, помноженої на коефіцієнт 0,4 - разом 80 балів, і додаткових 20 балів при опитуванні під час заліку. Студенти, які отримали при змістовому модульному контролі менше 60 балів до підсумкового семестрового контролю не допускаються.

Під час навчання студенти зобов'язані дотримуватися академічної доброчесності:

- самостійно виконувати навчальні завдання, завдання поточного та підсумкового контролю;

- дотримуватися норм законодавства про авторське право;

- приймати активну участь у навчальному процесі;

- не запізнюватися на заняття, не пропускати заняття без поважних причин;

- *самостійно і своєчасно вивчити матеріал пропущеного заняття;*
- *давати достовірну інформацію про результати власної навчальної діяльності.*
- *бути терпимим і доброзичливим до однокурсників та викладачів.*

Інформаційні ресурси:

https://zp.edu.ua
http://library.zp.edu.ua:8081/lib2web/DocSearchForm
http://e-library.zp.edu.ua
https://zp.edu.ua/kafedra-zahistu-informaciyi