МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Кафедра *«Захист інформації»*
(найменування кафедри)

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Менеджмент інформаційної безпеки
(назва навчальної дисципліни)

Освітня програма: *Безпека інформаційних і комунікаційних систем*
(назва освітньої програми)

Спеціальність: *125 Кібербезпека*
(найменування спеціальності)

Галузь знань: *12 Інформаційні технології*
(найменування галузі знань)

Ступінь вищої освіти: *Бакалавр*
(назва ступеня вищої освіти)

Затверджено на засіданні кафедри
«*Захист інформації*»
(найменування кафедри)

Протокол № ____ від ____ _____ 2020 р.

м. Запоріжжя 2020

<table>
<tr><th colspan="2">1. Загальна інформація</th></tr>
<tr><td>Назва дисципліни</td><td>ППН 08. Менеджмент інформаційної безпеки (обов'язкова дисципліна).</td></tr>
<tr><td>Рівень вищої освіти</td><td>Перший (бакалаврський) рівень</td></tr>
<tr><td>Викладач</td><td>Куцак Сергій Вікторович, старший викладач.</td></tr>
<tr><td>Контактна інформація викладача</td><td>Телефон кафедри: 0617698491, телефон викладача: 0978797858, e-mail викладача: kuzak@ukr.net.</td></tr>
<tr><td>Час і місце проведення навчальної дисципліни</td><td>Згідно розкладу занять викладачів кафедри</td></tr>
<tr><td>Обсяг дисципліни</td><td>Загальна кількість годин – 240, кількість кредитів ECTS – 8.
Розподіл годин та вид контролю:
<table>
<tr><td></td><td>Семестр – 6</td><td>Семестр –7</td><td>Разом</td></tr>
<tr><td>Кредитів ECTS</td><td>4</td><td>4</td><td>7</td></tr>
<tr><td>Лекції</td><td>28</td><td>30</td><td>58</td></tr>
<tr><td>Лабораторні роботи</td><td>14</td><td>14</td><td>28</td></tr>
<tr><td>Самостійна робота</td><td>78</td><td>76</td><td>154</td></tr>
<tr><td>Вид контролю</td><td>залік</td><td>екзамен</td><td></td></tr>
</table></td></tr>
<tr><td>Консультації</td><td>Згідно з графіком консультацій</td></tr>
<tr><th colspan="2">2. Пререквізити і постреквізити навчальної дисципліни</th></tr>
<tr><td colspan="2">Передумовами вивчення дисципліни «Менеджмент інформаційної безпеки» є знання отримані під час вивчення дисциплін: ППН 03 «Нормативно-правове і організаційне забезпечення інформаційної безпеки» (теми: Структура нормативно-законодавчої бази в галузі інформаційної безпеки (ІБ) України, Організаційно-правовий режим ІБ), ППН 06 «Захист інформації в банківській сфері та електронному бізнесі» (теми: Організація банківської безпеки, Безпека електронних платіжних систем), ППН 07 «Основи криптографії та стеганографії» (теми: Характеристика симетричних і асиметричних криптосистем, Поняття електронного підпису), ППН 09 «Антивірусні технології» (теми: Класифікація і основні властивості руйнівних програмних засобів, Характеристики та особливості використання сучасних антивірусних програм), ППН 10 «Захист програмного забезпечення» (теми: Міжнародні стандарти з опису життєвого циклу програмного забезпечення, Класифікація методів дублювання інформації, Поняття та основні компоненти технології HASP), ППВВ 04 «Методи та засоби технічного захисту інформації» (теми: Канали витоку чутливої інформації, Захист інформації від витоку технічними каналами), ППВВ 05 «Захищені мережні технології» (теми: Засоби забезпечення безпеки в обчислювальних мережах, Протоколи інформаційної безпеки, Технологія мережних екранів).
Компетентності:
КЗ 1. Здатність застосовувати знання в практичних ситуаціях.
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
КФ 2. Здатність впроваджувати принципи організаційного забезпечення і порядок формування політики безпеки на об'єктах інформаційної діяльності.
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 5. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 11. Здатність застосовувати методи та засоби криптографічного, стеганографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
КФ 12. Здатність виконувати моніторинг ресурсів і процесів функціонування, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</td></tr>
</table>

Знання, здобуті при вивченні дисципліни «Менеджмент інформаційної безпеки», є обов'язковими для вивчення дисципліни ППН 11 «Проектування, впровадження та супровід комплексних систем захисту інформації».

3. Характеристика навчальної дисципліни

Дисципліна «Менеджмент інформаційної безпеки» є базовою у підготовці фахівця з інформаційної безпеки, її вивчення дає можливість сформувати розуміння предметної області та професії, що безпосередньо пов'язані з управлінням захисту інформації і наданням фахової оцінки кіберінцидентам в інформаційно-комунікаційних системах.

Перелік компетентностей, яких набуває студент при вивченні дисципліни:

Загальні компетентності:

КЗ 1. Здатність застосовувати знання в практичних ситуаціях.

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

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

Фахові компетентності:

КФ 6. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 9. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 10. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

КФ 13. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.

Результати навчання:

ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

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 9. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН 10. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно- телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

ПРН 21. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН 23. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

ПРН 24. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно- телекомунікаційних (автоматизованих)

системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
ПРН 25. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН 26. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

4. Мета вивчення навчальної дисципліни

Метою викладання навчальної дисципліни «Менеджмент інформаційної безпеки» є формування комплексу знань щодо основ менеджменту інформаційної безпеки, набуття студентом теоретичних знань та практичних навичок щодо управління інформаційною безпекою в інформаційно-телекомунікаційних (автоматизованих) системах для реалізації встановленої політики безпеки.

5. Завдання вивчення дисципліни

Основними завданнями вивчення дисципліни «Менеджмент інформаційної безпеки» є формування у студентів комплексу знань щодо стану та тенденцій забезпечення безпеки інформаційних систем; орієнтування в основних сучасних поглядах на сутність інформаційної безпеки підприємства та держави; знати і вміти давати характеристику стану ІБ.

6. Зміст навчальної дисципліни

Навчальна дисципліна складається з чотирьох змістовних модулів:

1. *Концептуальні засади формування системи ІБ.*
2. *Стандартизація підходів до забезпечення ІБ.*
3. *Управління ризиками в сфері ІБ.*
4. *Менеджмент інцидентів ІБ.*

7. План вивчення навчальної дисципліни

№ тижня	Назва теми	Форми організації навчання	Кількість годин
1, 2	*Основні положення ІБ. Концепція інформаційної безпеки організації. Концепція національної безпеки України.*	*лекція* *лаб. робота* *сам. робота*	4 2 10
3, 4	*Класифікація загроз ІБ. Вибір стратегії зменшення загроз ІБ. Політика кібербезпеки інформації та модель порушника.*	*лекція* *лаб. робота* *сам. робота*	4 2 14
5 – 7	*Методи і засоби забезпечення ІБ: основні принципи, фактори і способи. Задачі забезпечення цілісності, доступності, конфіденційності та приватності.*	*лекція* *лаб. робота* *сам. робота*	5 4 15
8 – 10	*Поняття та категоризація державних інформаційних ресурсів. Загрози інформації та вибір функціонального класу послуг захисту.*	*лекція* *лаб. робота* *сам. робота*	5 2 15
11, 12	*Оціночні стандарти в інформаційній безпеці. Стандарти управління інформаційною безпекою BS 7799 і ISO/IEC 17799.*	*лекція* *лаб. робота* *сам. робота*	4 2 12
13 – 15	*Етапи розробки і впровадження системи управління ІБ. Планування безперебійної роботи підприємства. Безперервний внутрішній аудит ІБ підприємства.*	*лекція* *лаб. робота* *сам. робота*	6 2 12
16 – 18	*Основні поняття про систему управління ризиками. Метод оцінки ризиків на основі моделі загроз і вразливостей. Метод оцінки ризиків на основі моделі інформаційних потоків.*	*лекція* *лаб. робота* *сам. робота*	6 4 14
19 – 21	*Якісні і кількісні методики управління ризиками. Ідентифікація ресурсів і побудова моделі системи з точки зору ІБ.*	*лекція* *лаб. робота* *сам. робота*	6 2 14

22 – 24	*Сценарій аналізу інформаційних ризиків компанії. Табличні методи оцінки ризиків. Сучасні методи управління ризиками ІБ.*	*лекція* *лаб. робота* *сам. робота*	6 2 16
25 – 28	*Концепція побудови ефективної системи менеджменту інцидентів ІБ. Класифікація і архітектура системи виявлення та блокування атак.*	*лекція* *лаб. робота* *сам. робота*	8 4 20
29, 30	*Характеристика діяльності груп CERT/CSIRT. Етапи створення груп CERT/ CSIRT. Єдина система CIRT та державний центр безпеки.*	*лекція* *лаб. робота* *сам. робота*	4 2 12
		Разом	***240***

8. Самостійна робота

Самостійна робота включає в себе: вивчення теоретичного матеріалу, підготовку до лабораторних робіт, підготовку до рубіжного та підсумкового контролю.

№ з/п	Назва теми, що виноситься на самостійну роботу	Кількість годин
1	*Концепція інформаційної безпеки організації.*	12
2	*Класифікація вразливостей безпеці інформації.*	12
3	*Основи організаційного та інженерно-технічного захисту*	12
4	*Міжнародний стандарт ISO/IEC 15408.*	14
5	*Сертифікація СУІБ на відповідність ISO 27001.*	14
6	*Зміст етапів розробки та впровадження системи управління ІБ.*	12
7	*Метод оцінки ризиків на основі моделі інформаційних потоків.*	14
8	*Метод CRAMM. Ідентифікація ресурсів і побудова моделі системи.*	12
9	*Методи оцінювання інформаційних ризиків.*	14
10	*Методика OCTAVE, Risk Watch та Oracle Crystal Ball.*	12
11	*Основні етапі ефективного менеджменту інцидентів ІБ.*	14
12	*Загальна характеристика тематичного розмежування доступу.*	12
	Разом	***154***

9. Система та критерії оцінювання курсу

Під час вивчення дисципліни «Менеджмент інформаційної безпеки» передбачені наступні види контролю: поточний, рубіжний, семестровий контроль (з урахуванням відвідування занять, виконання лабораторних робіт, тестування при здачі модулів).

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

Для оцінювання студентів використовується система накопичування балів. Підсумкова оцінка з дисципліни виставляється за 100-бальною шкалою, з наступним переведенням в національну шкалу та шкалу ECTS.

Бали нараховуються та розподіляються за наступною схемою: виконання аудиторних завдань, лабораторних та контрольних робіт в підсумку оцінюється в 60 балів, тестова робота на знання теоретичного матеріалу оцінюється в 40 балів.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	*Оцінка ECTS*	*Оцінка за національною шкалою*	
		Для екзамену	*Для заліку*
90 – 100	***A***	*відмінно*	*зараховано*
85-89	***B***	*добре*	
75-84	***C***		
70-74	***D***	*задовільно*	
60-69	***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

Під час вивчення дисципліни «Менеджмент інформаційної безпеки» студенти зобов'язані:

1. *Відвідувати навчальні заняття, передбачені розкладом (або вчасно інформувати про неможливість відвідування).*
2. *Відповідально, сумлінно і творчо ставитися до виконання навчальних завдань.*
3. *Діяти у професійних і навчальних ситуаціях із позицій академічної доброчесності та професійної етики:*
   - *усвідомлювати значущість норм академічної доброчесності;*
   - *самостійно виконувати навчальні завдання;*
   - *коректно посилатися на джерела інформації у разі запозичення ідей, тверджень, відомостей;*
4. *Бути терплячими і доброзичливими до однокурсників та викладачів.*

Викладач та всі здобувачі, що вивчають цей курс, зобов'язуються дотримуватись Законів України «Про освіту» та «Про вищу освіту», Статуту та Правил внутрішнього розпорядку Університету, «Положення про організацію освітнього процесу в Національному університеті «Запорізька політехніка»», етичних норм, та розуміють, що за їх порушення несуть особисту відповідальність.