МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Кафедра *«Захист інформації»*
(найменування кафедри)

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Нормативно-правове і організаційне забезпечення 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

1. Загальна інформація

Назва дисципліни	*ППН 03. Нормативно-правове і організаційне забезпечення інформаційної безпеки (обов'язкова дисципліна).*
Рівень вищої освіти	*Перший (бакалаврський) рівень*
Викладач	*Куцак Сергій Вікторович, старший викладач.*
Контактна інформація викладача	*Телефон кафедри: 0617698491, телефон викладача: 0978797858, e-mail викладача: kuzak@ukr.net.*
Час і місце проведення навчальної дисципліни	*Згідно розкладу занять викладачів кафедри*
Обсяг дисципліни	*Загальна кількість годин – 210, кількість кредитів ECTS – 7.* *Розподіл годин та вид контролю:*

	Семестр – 2	*Семестр –3*	***Разом***
Кредитів ECTS	*3*	*4*	***7***
Лекції	*14*	*30*	***44***
Практичні заняття	*14*	*14*	***28***
Самостійна робота	*62*	*76*	***138***
Вид контролю	*залік*	*екзамен*	

Консультації	*Згідно з графіком консультацій*

2. Пререквізити і постреквізити навчальної дисципліни

Передумовами вивчення дисципліни «Нормативно-правове і організаційне забезпечення інформаційної безпеки» є знання отримані під час вивчення дисципліни ППН 02 «Інформаційна діяльність та кібербезпека» (теми: Архітектура типових персональних комп'ютерів, Апаратне забезпечення локальних обчислювальних мереж, Безпека комп'ютерних мереж) та шкільного курсу Правознавства.

Компетентності:

КЗ 1. Здатність застосовувати знання в практичних ситуаціях.

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

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

Знання, здобуті при вивченні дисципліни «Нормативно-правове і організаційне забезпечення інформаційної безпеки», є обов'язковими для вивчення дисциплін: ППН 06 «Захист інформації в банківській сфері та електронному бізнесі», ППН 08 «Менеджмент інформаційної безпеки» ППН 11 «Проектування, впровадження та супровід комплексних систем захисту інформації».

3. Характеристика навчальної дисципліни

Дисципліна «Нормативно-правове і організаційне забезпечення 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 організацією захисту і наданням правової 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 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.

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 12. Розробляти моделі загроз та порушника.

ПРН 18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах (ІТС).

ПРН 22. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

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 «Нормативно-правове і організаційне забезпечення інформаційної безпеки» є отримання студентами знань з питань законодавчого забезпечення діяльності у сфері захисту інформації з обмеженим доступом і отримання практичних навиків застосування організаційних заходів, направлених на захист інформації.

5. Завдання вивчення дисципліни

Основними завданнями вивчення дисципліни «Нормативно-правове і організаційне забезпечення інформаційної безпеки» є закладення у студентів знань та умінь застосовувати діючу законодавчу базу в галузі інформаційної безпеки (ІБ), необхідних для професійної діяльності, включаючи вміння впроваджувати організаційні заходи на об'єктах інформаційної діяльності (ОІД) на підприємствах та установах різної форми власності.

6. Зміст навчальної дисципліни

Навчальна дисципліна складається з чотирьох змістовних модулів:

1. *Доктрина інформаційної безпеки України.*
2. *Нормативно-правове управління забезпеченням ІБ.*
3. *Організаційно-правовий режим ІБ.*
4. *Реалізація організаційних методів та заходів забезпечення ІБ.*

7. План вивчення навчальної дисципліни

№ тижня	Назва теми	Форми організації навчання	Кількість годин
1, 2	*Вступ. Мета, завдання і зміст дисципліни. Основні визначення: правові, нормативні та відомчі документи.*	*лекція* *прак. заняття* *сам. робота*	2 2 8
3, 4	*Структура нормативно-законодавчої бази в галузі ІБ України. Концепція кібербезпеки України. Відповідальність за порушення законодавства про захист інформації.*	*лекція* *прак. заняття* *сам. робота*	2 2 10

5 – 7	*Статті Кримінального Кодексу України стосовно комп'ютерних злочинів. Конвенція Ради Європи про кіберзлочинність. Основні завдання Кіберполіції України.*	*лекція* *прак. заняття* *сам. робота*	4 4 12
8 – 10	*Нормативні документи в галузі технічного захисту інформації (НД ТЗІ). Правове регулювання захисту інформації в автоматизованих системах.*	*лекція* *прак. заняття* *сам. робота*	2 2 12
11, 12	*Ліцензійна та сертифікаційна діяльність у галузі захисту інформації. Правова регламентація охоронної діяльності.*	*лекція* *прак. заняття* *сам. робота*	2 2 10
13 – 15	*Інформаційне право окремих країн світу. Міжнародні правові документи у сфері інформаційної безпеки. Міжнародні стандарти в галузі ІБ.*	*лекція* *прак. заняття* *сам. робота*	2 2 10
16 – 18	*Особливості організаційних методів ІБ. Формування організаційно-правового режиму ІБ. Розробка політики безпеки.*	*лекція* *прак. заняття* *сам. робота*	6 4 14
19 – 21	*Поняття комплексної системи захисту інформації (КСЗІ). Категорування ресурсів в ІТС. Регламентація доступу до ОІД*	*лекція* *прак. заняття* *сам. робота*	6 2 14
22 – 24	*Управління механізмами захисту. Організація доступу до інформаційних ресурсів ІТС. Оцінка ефективності КСЗІ.*	*лекція* *прак. заняття* *сам. робота*	6 2 16
25 – 28	*Вибір показників ефективності і критеріїв оптимальності КСЗІ. Попередні випробування, дослідна експлуатація, державна експертиза та супровід КСЗІ. Атестація виділених приміщень. Поняття акту обстеження.*	*лекція* *прак. заняття* *сам. робота*	8 4 20
29, 30	*Задачі і складові частини секретного діловодства: документування і організація документообігу. Підбір і підготовка персоналу.*	*лекція* *прак. заняття* *сам. робота*	4 2 12
		Разом	***210***

8. Самостійна робота

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

№ з/п	Назва теми, що виноситься на самостійну роботу	Кількість годин
1	*Основи інформаційного права*	7
2	*Законодавство України у галузі інформаційної безпеки*	8
3	*Захист державної та комерційної таємниці*	7
4	*Характеристика кіберзлочинів: правовий аспект*	8
5	*Загальна характеристика нормативних документів ТЗІ*	8
6	*Сертифікація діяльності в сфері захисту інформації*	9
7	*Регламентація охоронної діяльності*	8
8	*Міжнародне співробітництво у сфері кібернетичної безпеки*	7
9	*Алгоритм і етапи практичних заходів зі створення системи захисту*	5
10	*Види стратегій захисту інформації*	6
11	*Перелік нормативних документів з організації КСЗІ*	6
12	*Рівні політики безпеки та їх характеристики*	8
13	*Зарубіжні стандарти розробки політик ІБ*	7
14	*Структурне представлення організаційно-правового захисту*	8
15	*Порядок розробки моделі об'єкту захисту*	5
16	*Види дозволів на право допуску до конфіденційної інформації.*	6
17	*Порядок допуску на контрольовану зону*	5

18	*Класифікація ідентифікаторів власника*	8
19	*Робота з документами з « Переліку службової інформації»*	7
20	*Робота з документами, що містять державну таємницю*	5
	Разом	***138***

9. Система та критерії оцінювання курсу

Під час вивчення дисципліни «Нормативно-правове і організаційне забезпечення інформаційної безпеки» передбачені наступні види контролю: поточний, рубіжний, семестровий контроль (з урахуванням відвідування занять, виконання практичних завдань, 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, практичних 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 «Нормативно-правове і організаційне забезпечення 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.