МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Кафедра *«Захист інформації»*
(найменування кафедри)

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в банківській сфері та електронному бізнесі
(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 06. Захист інформації в банківській сфері та електронному бізнесі (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 – 240, кількість кредитів ECTS – 8. Розподіл годин та вид контролю:*

	Семестр – 4	*Семестр –5*	***Разом***
Кредитів ECTS	*4*	*4*	***8***
Лекції	*30*	*30*	***60***
Практичні заняття	*14*	*14*	***28***
Самостійна робота	*76*	*76*	***152***
Вид контролю	*залік*	*екзамен*	

Консультації	*Згідно з графіком консультацій*

2. Пререквізити і постреквізити навчальної дисципліни

Передумовами вивчення дисципліни «Захист інформації в банківській сфері та електронному бізнесі» 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), 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 05 «Телекомунікаційні та комп'ютерні мережі» (теми: Сучасні телекомунікаційні технології, Протоколи передачі даних), ППВВ 04 «Методи та засоби технічного захисту інформації» (теми: Канали витоку чутливої інформації, Захист інформації від витоку технічними каналами).

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 11. Здатність застосовувати методи та засоби криптографічного, стеганографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

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

3. Характеристика навчальної дисципліни

Дисципліна «Захист інформації в банківській сфері та електронному бізнесі» 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 банківській сфері та електронному бізнесі, які використовують 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 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.

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 5. Здатність забезпечувати неперервність бізнесу згідно 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 7. Аналізувати економічну ефективність заходів інформаційної безпеки, застосовувати основні засади охорони праці та безпеки життєдіяльності.
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 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
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 22. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
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 26. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

ПРН 30. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

4. Мета вивчення навчальної дисципліни

Метою викладання навчальної дисципліни «Захист інформації в банківській сфері та електронному бізнесі» є отримання студентами знань з питань забезпечення інформаційної безпеки (ІБ) діяльності фінансових установ та комерційних підприємства всіх форм власності та отримання практичних навиків по організації робіт, направлених на захист інтересів підприємства від зовнішніх і внутрішніх загроз.

5. Завдання вивчення дисципліни

Основними завданнями вивчення дисципліни «Захист інформації в банківській сфері та електронному бізнесі» є формування у студентів системного підходу до вирішення проблем побудови системи безпеки, що забезпечує захищену та стабільну роботу банківських установ та комерційних підприємств, що використовують інформаційно-телекомунікаційні системи..

6. Зміст навчальної дисципліни

Навчальна дисципліна складається з чотирьох змістовних модулів:

1. *Проблеми безпеки банківської діяльності.*
2. *Забезпечення безпеки банківської діяльності.*
3. *Основні напрями електронної комерції.*
4. *Безпека електронної комерції.*

7. План вивчення навчальної дисципліни

№ тижня	Назва теми	Форми організації навчання	Кількість годин
1, 2	*Предмет, задачі та зміст дисципліни. Загальні питання банківської діяльності. Управління комерційним банком.*	*лекція* *прак. заняття* *сам. робота*	4 2 10
3, 4	*Загрози безпеці фінансово-кредитним установам. Ризик втрати інформації з обмеженим доступом. Ризики, пов'язані з формуванням дезінформації та інформаційно-психологічним впливом.*	*лекція* *прак. заняття* *сам. робота*	4 2 14
5 – 7	*Система безпеки комерційного банку, її структура і функції. Організація роботи служби безпеки комерційного банку. Система економічної розвідки банку*	*лекція* *прак. заняття* *сам. робота*	6 4 15
8 – 10	*Національне законодавство в банківській сфері. Стандарти НБ. Міжнародні стандарти для системи управління інформаційною безпекою банку. Забезпечення безпеки кредитних операцій.*	*лекція* *прак. заняття* *сам. робота*	6 2 14
11, 12	*Особливості забезпечення інформаційної безпеки комерційного банку. Характеристика сучасних автоматизованих банківських систем (АБС).*	*лекція* *прак. заняття* *сам. робота*	4 2 12
13 – 15	*Організація захисту від можливих атак на різні компоненти АБС. Організація допуску до ресурсів АБС. Захист електронних банківських документів.*	*лекція* *прак. заняття* *сам. робота*	6 2 12
16 – 18	*Технологія Big Data для бізнесу. Електронні торгові майданчики: класи (категорії) ведення електронної комерції. Характеристики основних електронних торговельних майданчиків моделей B2C, B2B, B2G, G2B.*	*лекція* *прак. заняття* *сам. робота*	6 4 14

19 – 21	*Інформаційні системи для автоматизації роботи в соціальних мережах і блогах. Соціальні мережі в підприємництві і бізнесі.*	*лекція* *прак. заняття* *сам. робота*	6 2 14
22 – 24	*Визначення електронного платежу і електронної платіжної системи. Платіжні валюти (електронні валюти). Білінг. Електронні платіжні інструменти.*	*лекція* *прак. заняття* *сам. робота*	6 2 15
25 – 28	*Типовий сценарій торгової інформаційної мережі класу B2B. Характеристика електронного обміну даними (ЕОД). Схема ЕОД-взаємодії підприємств великого та малого бізнесу. Стандарт UN / EDIFACT.*	*лекція* *прак. заняття* *сам. робота*	8 4 20
29, 30	*Безпека роботи в соціальних мережах. Безпека при використанні мобільних пристроїв. Застосування технологій NFC і HCE. Відповідальність за безпеку електронних платежів. Протокол безпеки 3D-Secure.*	*лекція* *прак. заняття* *сам. робота*	4 2 12
		Разом	***240***

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	*Контрольно-наглядові функції Національного банку України*	*5*
2	*Організація міжбанківських розрахунків.*	*6*
3	*Шахрайство при здійсненні банківських операцій*	*8*
4	*Правовий захист банківських інтересів і банківської таємниці*	*7*
5	*Охорона стаціонарних об'єктів і перевезень комерційного банку*	*9*
6	*Безпека банківських платіжних карт*	*6*
7	*Безпека касових операцій*	*7*
8	*Система Клієнт-Банк*	*6*
9	*Захист електронних банківських платежів*	*10*
10	*Комплекс надання електронних довірчих послуг MASTERKEY*	*8*
11	*Internet і Web – основні технології електронної комерції*	*6*
12	*Сучасні технології електронної комерції*	*9*
13	*Державні електронні торгові майданчики*	*8*
14	*Соціальний медіамаркетинг в соціальних мережах*	*9*
15	*Правові основи електронної торгівлі*	*7*
16	*Структура обміну повідомленнями в стандарті EANCOM*	*9*
17	*Вітчизняні електронні платіжні системи і їх характеристика*	*7*
18	*Безпека при використанні мобільних пристроїв: NFC та HCE*	*9*
19	*Заходи безпеки при оплаті товарів або послуг в Інтернет-магазині*	*10*
20	*Довірені організації та служби для підвищення безпеки електрон. комер.*	*6*
	Разом	***152***

9. Система та критерії оцінювання курсу

Під час вивчення дисципліни «Захист інформації в банківській сфері та електронному бізнесі» 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 «Захист інформації в банківській сфері та електронному бізнесі» 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.