МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***обов'язкова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки
та інформаційних технологій *Ольга СТАРКОВА*

Харків
2022

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 1 від 27.08.2022 р.

Розробники:
Солодовник Г.В., доцент кафедри КІТ
Литвиненко Є.М., старший викладач кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Організаційні заходи відіграють важливу роль у створенні надійного механізму захисту інформації, так як можливості несанкціонованого використання конфіденційних відомостей найчастіше обумовлені не тільки технічними аспектами, а й зловмисними діями, а також недбальством, недбалістю, халатністю користувачів або обслуговуючого персоналу, що ігнорує елементарні правила захисту. Закони та нормативні акти виконуються тільки в тому випадку, якщо вони підкріплюються організаторською діяльністю відповідних структур, що створюються в державі, відомствах, установах і організаціях. Під час розгляду питань захисту інформації така діяльність розглядається як організаційні методи забезпечення. В інформаційних системах організаційні заходи виконують стрижневу роль в реалізації комплексної системи захисту інформації. Тільки за їх допомогою можливе об'єднання на правовій основі інженерно-технічних, програмно-апаратних, криптографічних та інших засобів захисту інформації в єдину комплексну систему.

Предметом вивчення дисципліни є процедури, методи та засоби організаційного забезпечення діяльності щодо інформаційної безпеки.

Об'єктом вивчення дисципліни є організаційне забезпечення захисту інформації.

Мета навчальної дисципліни «Організаційне забезпечення захисту інформації» – формування теоретичних знань щодо організаційного забезпечення діяльності з захисту інформації, такої як: аналіз і оцінка інформаційної безпеки об'єкта щодо його організаційного забезпечення; організації керування загрозами; реагування на інциденти; організації і забезпечення режиму таємності; підбору, розстановки і роботи з кадрами.

Результатами вивчення дисципліни є отримання знань, вмінь та навичок з організаційного забезпечення діяльності з захисту інформації, такої як: аналіз і оцінка інформаційної безпеки об'єкта щодо його організаційного забезпечення; організації керування загрозами; реагування на інциденти; організації і забезпечення режиму таємності; підбору, розстановки і роботи з кадрами.

Характеристика навчальної дисципліни

Курс	**4**
Семестр	**7**
Кількість кредитів ECTS	**4**
Форма підсумкового контролю	**екзамен**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Основи математичного моделювання	Переддипломна практика
Комплексні системи захисту інформації	Дипломний проєкт

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КЗ 1. Здатність застосовувати знання у 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.	РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.	РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.	РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.	РН 4 – 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.
КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.	РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

КЗ 2. Знання та розуміння предметної області та розуміння професії.	РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. 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.	РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. 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.	РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
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 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	
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 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 12. Здатність аналізувати,	РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	
КЗ 2. Знання та розуміння предметної області та розуміння професії. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 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.

КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 29 – 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.
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно	РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

встановленої політики інформаційної та/або кібербезпеки.	
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 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
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 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати	РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	

КЗ 1. Здатність застосовувати знання у практичних ситуаціях. 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 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

КЗ 2. Знання та розуміння предметної області та розуміння професії. 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 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

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 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 44 – вирішувати задачі забезпечення безперервності бізнеспроцесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 45 – застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та	РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних	РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.

(автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.	РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Програма навчальної дисципліни

Змістовий модуль 1. Роль організаційного забезпечення при здійсненні захисту інформації

Тема 1. Завдання організаційного забезпечення захисту інформації.

Тема 2. Організаційні основи захисту інформації.

Тема 3. Аналіз і оцінка загроз інформаційної безпеки об'єкта щодо його організаційного забезпечення.

Тема 4. Організація керування загрозами.

Тема 5. Контроль доступу.

Змістовий модуль 2. Організація доступності активів і робота з персоналом

Тема 6. Організація доступності.

Тема 7. Реагування на інциденти.

Тема 8. Підбір, розстановка і робота з кадрами.

Тема 9. Організація і забезпечення режиму таємності.

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці «Рейтинг-план навчальної дисципліни».

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються лекції (теми 1-9), презентації (теми 1-9), лабораторні роботи (теми 1-8).

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що надає студенту допуск до екзамену, – 35 балів);

2) підсумковий/семестровий контроль, що проводиться у формі екзамену, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

– вміння застосовувати законодавчу та нормативно-правову базу України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

– вміння виявляти, ідентифікувати, аналізувати та реагувати на інциденти інформаційної і/або кібербезпеки;

– вміння керувати загрозами, що виникають під час інформаційної діяльності підприємств та організацій;

– вміння аналізувати засоби безпеки, що пропонуються до впровадження;

– вміння формувати та організовувати роботу служби захисту інформації та груп реагування на інциденти та катастрофи;

– вміння оцінювати загрозу надлишкової та залишкової інформації що зберігається у відкритому доступі у глобальних комп’ютерних мережах.

За дисципліною передбачені такі методи поточного формативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення студентами виконаних лабораторних завдань.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Лекційні заняття: в технологічній карті бали на цей вид робіт не виділені.

Лабораторні заняття: максимальна кількість балів становить 60 (виконання та захист лабораторних робіт – 60), а мінімальна – 35.

Самостійна робота: складається з часу, який здобувач витрачає на вивчення нового матеріалу, на підготовку до виконання лабораторних робіт та на підготовку до екзамену, в технологічній карті бали на цей вид робіт не виділені.

Підсумковий контроль: проводиться у вигляді екзамену, максимальна кількість балів становить 40. Мінімальна умова допуску до екзамену – отримання мінімального балу за лабораторні роботи (35). В разі не виконання плану лабораторних робіт студент до екзамену

вважається не допущеним.

Загальна сума балів підсумкової/семестрової перевірки успішності складається з балів за лекційні заняття, лабораторні роботи і екзамен. Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: «60 і більше балів – зараховано», «59 і менше балів – не зараховано» та заноситься у залікову «Відомість обліку успішності» навчальної дисципліни.

Форми оцінювання та розподіл балів наведено у таблиці «Рейтинг-план навчальної дисципліни».

Рейтинг-план навчальної дисципліни

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1	***Аудиторна робота***			
	Лекція	Завдання організаційного забезпечення захисту інформації		
	Лабораторне заняття	Лабораторна робота №1. Робота з Центрами сертифікації безпеки	Виконання лабораторної роботи	
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Тема 2	***Аудиторна робота***			
	Лекція	Організаційні основи захисту інформації		
	Лабораторне заняття	Лабораторна робота №1 (продовження).	Захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Т	***Аудиторна робота***			

Тема 3	Лекція	Аналіз і оцінка загроз інформаційної безпеки об'єкта щодо його організаційного забезпечення		
	Лабораторне заняття	Лабораторна робота №2. Аналіз інформації про технічне забезпечення організації, що знаходиться у відкритому доступі	Виконання та захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Тема 4	***Аудиторна робота***			
	Лекція	Організація керування загрозами		
	Лабораторне заняття	Лабораторна робота №3. Аналіз сертифікатів безпеки сайтів організацій	Виконання та захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Тема 5	***Аудиторна робота***			
	Лекція	Контроль доступу		
	Лабораторне заняття	Лабораторна робота №4. Моніторинг інформації, яка залишається у відкритому доступі, після ліквідації веб-ресурсів	Виконання лабораторної роботи	
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Тем	***Аудиторна робота***			
	Лекція	Організація доступності		

а 6	Лабораторне заняття	Лабораторна робота №4 (продовження).	Захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Т е м а 7	***Аудиторна робота***			
	Лекція	Реагування на інциденти		
	Лабораторне заняття	Лабораторна робота №5. Перевірка наявності службової інформації організації у відкритому доступі, після ліквідації веб-ресурсів	Виконання та захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Т е м а 8	***Аудиторна робота***			
	Лекція	Підбір, розстановка і робота з кадрами		
	Лабораторне заняття	Лабораторна робота №6. Організація роботи по брендуванню організації	Виконання та захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Т е м а 9	***Аудиторна робота***			
	Лекція	Організація і забезпечення режиму таємності		
	Самостійна робота			
	Питання та завдання до самостійного	Вивчення лекційного матеріалу.		

	опрацювання			
Екзамен				40

Рекомендована література

Основна

1. Інформаційна безпека / за ред. Ю.Я.Бобала, І.В. Горбатого. Львів : Львівська політехніка, 2019. 580 с.

2. Хорошко В.О. Проектування комплексних систем захисту інформації. Львів : Львівська політехніка, 2020. 320 с.

3. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Львів: Магнолія, 2018. – 320 с.

4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : підручник. Львів : Магнолія 2006, 2020. 448 с.

5. Лісовська Ю. П. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2021. 272 с.

6. Остапов С. Е. Кібербезпека: сучасні технології захисту : навч. посіб. Львів : Новий Світ-2000, 2021. 679 с.

Додаткова

1. Комаров М. Ю. Огляд кібератак на об'єкти критичної інфраструктури // Електронне моделювання. 2019. No 6. С. 91-106.

2. Ibrahimova A. Z. Information security and influencing factors // Право України. 2021. No 11. С. 234-244.

3. Розвиток моделей кібератак у площині інформаційної безпеки підприємства / Є. М. Галахов, В. В. Собчук // Телекомунікаційні та інформаційні технології. 2019. No 4. С. 12-24.

Інформаційні ресурси

1. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі». Київ : Департамент спеціальних телекомунікаційних систем та 11 захисту інформації Служби безпеки України. 2000. [Електронний ресурс]. Режим доступу : http://www.dut.edu.ua/uploads/l_1023_75718671.pdf

2. ДСТУ 3396.1-96. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Режим доступу : https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf

3. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною «Організаційне забезпечення захисту інформації» https://pns.hneu.edu.ua/course/view.php?id=8976.