

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи



Жаріна НЕМАТІКАЛО

ВСТУП ДО ФАХУ
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:

Старкова О.В., професор кафедри КІТ

Мерлак О.В., 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

Вступ до фаху – нормативна дисципліна, яка розкриває можливості, напрями діяльності, необхідність кібербезпеки. Кібербезпека – дискусійна сфера діяльності. Деякі джерела звужують його сферу застосування, стверджуючи, що насправді це лише частина інформаційної безпеки, яка стосується лише середовища комп'ютерних мереж (іноді навіть згадується лише Інтернет). А інші, навпаки, розширюють тему кібербезпеки, і мають для цього підстави – адже кіберпростір охоплює комп'ютерні мережі, і всі пристрої, які в цих мережах працюють, і всю комп'ютерну техніку, і людей, які використовують ці технології та пристрої.

Предметом вивчення дисципліни є базові визначення та поняття кібербезпеки, методології, методи, способи кібербезпеки.

Об'єктами вивчення виступають основні поняття та термінологія кібербезпеки, сфери інформаційної безпеки.

Мета навчальної дисципліни – досягнення фундаментального уявлення про сутність спеціальності, правила та принципи роботи в інформаційному середовищі, вміння застосовувати відповідні методології, методи, способи під час вирішення завдань професійної діяльності.

Результатами вивчення дисципліни є надбання вміння і навичок із застосування правил та принципів роботи в інформаційному середовищі, відповідних методологій, методів, способів під час вирішення завдань професійної діяльності.

Характеристика навчальної дисципліни

Курс	1
Семестр	1
Кількість кредитів ECTS	5,5
Форма підсумкового контролю	залік

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Інформатика за шкільною програмою	Технології програмування
Математика за шкільною програмою	Розробка та аналіз алгоритмів

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.

<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ 2. Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.</p>	<p>РН 2 – організувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.</p>
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ 2. Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.</p>	<p>РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.</p>
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ 2. Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.</p>	<p>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.</p>
<p>КЗ 2. Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.</p>	<p>РН 5 – адаптуватися в умовах частой зміни технологій професійної діяльності, прогнозувати кінцевий результат.</p>
<p>КЗ 2. Знання та розуміння предметної області та розуміння професії.</p>	<p>РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.</p>
<p>КЗ 2. Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної</p>	<p>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.</p>

<p>діяльності в галузі інформаційної та/або кібербезпеки.</p>	
<p>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.</p>	<p>РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.</p>
<p>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. 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</p>	<p>РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.</p>

<p>впровадженій системи управління інформаційною та/або кібербезпекою.</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>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.</p>	
<p>КЗ 2. Знання та розуміння предметної області та розуміння професії.</p> <p>КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</p> <p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення</p>	<p>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.</p>

<p>кібератак, збоїв та відмов різних класів та походження.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p>	
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p>	<p>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).</p>
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p>	<p>РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.</p>

<p>КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p>	
<p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>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.</p>	<p>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.</p>

<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p>	<p>РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.</p>
<p>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.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>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.</p>	<p>РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.</p>

<p>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.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>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.</p>	<p>РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.</p>
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>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.</p> <p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p>	<p>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 та/або кібербезпеки.</p>

<p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>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.).</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>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.</p>	
<p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p>	<p>РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.</p>

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

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 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

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.

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 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

<p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>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.</p>	<p>РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.</p>
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</p> <p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p>	<p>РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.</p>

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.

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. Структура IoT

Тема 1. Потреба у кібербезпеці.

Тема 2. Куб кібербезпеки.

Тема 3. Атаки: поняття та методи.

Тема 4. Захист даних і конфіденційність.

Змістовий модуль 2. Методики захисту

Тема 5. Методики захисту інформації.

Тема 6. Забезпечення цілісності даних.

Тема 7. Захист організації.

Тема 8. Дослідження професії кібербезпеки.

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 2-8), презентації (теми 2-8), 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 – 100 балів; мінімальна сума – 60 балів);

2) підсумковий/семестровий контроль, що проводиться у формі заліку, 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 розуміти термінологію, напрями діяльності, пояснювати поняття, методики та проблеми кібербезпеки;
- вміння досліджувати дії в Інтернеті, що можуть скомпрометувати безпеку чи конфіденційність;
- вміння виконувати шифрування повідомлень;
- вміння використовувати програму хешування для перевірки цілісності даних;
- вміння використовувати цифровий підпис, розуміти концепцію цифрового підпису;
- вміння створювати надійні паролі, розуміти концепцію надійного пароля.

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, контроль самостійного виконання індивідуального завдання.

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 100 (виконання та захист лабораторних робіт – 100), а мінімальна – 60.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до експрес-опитувань за лекціями, в технологічній карті бали на цей вид робіт не виділені.

Підсумковий контроль: проводиться у вигляді заліку, максимальна кількість балів становить 100. Мінімальна умова отримання заліку – наявність мінімального балу за лабораторні роботи (60). В разі не виконання плану лабораторних робіт студент до заліку вважається не допущеним.

Загальна сума балів підсумкової/семестрової перевірки успішності складається з балів за лабораторні роботи. 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	Мак бал
Тема 1	<i>Аудиторна робота</i>			
	Лекція	Потреба у кібербезпеці		
	Лабораторне заняття	Лабораторна робота №1. Світ кібербезпеки	Виконання та захист лабораторної роботи	10
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Тема	<i>Аудиторна робота</i>			
	Лекція	Куб кібербезпеки		

а 2	Лабораторне заняття	Лабораторна робота №2. Захист особистих даних в соціальних мережах	Виконання та захист лабораторної роботи	10
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Т е м а 3	<i>Аудиторна робота</i>			
	Лекція	Атаки: поняття та методи		
	Лабораторне заняття	Лабораторна робота №3. Шифрування даних	Виконання та захист лабораторної роботи	15
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Т е м а 4	<i>Аудиторна робота</i>			
	Лекція	Захист даних і конфіденційність		
	Лабораторне заняття	Лабораторна робота №4. Порівняння даних за допомогою хешу	Виконання лабораторної роботи	
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Т е м а 5	<i>Аудиторна робота</i>			
	Лекція	Методики захисту інформації		
	Лабораторне заняття	Лабораторна робота №4. (продовження).	Захист лабораторної роботи	15

	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання лабораторної роботи		
Т е м а 6	Аудиторна робота			
	Лекція	Забезпечення цілісності даних		
	Лабораторне заняття	Лабораторна робота №5. Використання цифрового підпису	Виконання та захист лабораторної роботи	20
	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	Захист організації		
	Лабораторне заняття	Лабораторна робота №6. Створення паролей	Виконання та захист лабораторної роботи	15
	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	Дослідження професії кібербезпеки		
	Лабораторне заняття	Лабораторна робота №6. Дослідження ризиків	Виконання та захист лабораторної роботи	15
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Вивчення лекційного матеріалу. Підготовка до виконання лабораторної роботи. Виконання		

Рекомендована література

Основна

1. Brooks C. J., Grow, C., Craig, P., & Short, D. Cybersecurity essentials. John Wiley & Sons, 2018. 767 p.
0. Марущак А. І. Проблеми розслідування кіберзлочинів в Україні // Економіка, фінанси, право. 2018. No 1. С. 23-27.
0. Богуш В.М., Богуш В.В. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. Київ : Ліра-К, 2020. 552 с.
0. Aumasson J.-P. Serious Cryptography. A Practical Introduction to Modern Encryption. No Starch Press. 2018. 434p.
1. Seacord R.C. Effective C. An introduction to Professional C Programming. No Starch Press, 2020. 305p.

Додаткова

1. Половенко Л. П., Мерінова С. В. Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві // Підприємництво та інновації. – 2019. No 10. С. 183-187.
2. Chio C., Freeman D. Machine learning and security: Protecting systems with data and algorithms. " O'Reilly Media, Inc.", 2018. 385p.
3. Bowne S. Hands-On Cryptography with Python. Packt. 2018. 124 p.

Інформаційні ресурси

1. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною «Вступ до фаху» <https://pns.hneu.edu.ua/course/view.php?id=8971>.