

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

"ЗАТВЕРДЖУЮ"

Проректор з навчально-методичної роботи

Карина НЕМАШКАЛО

БЕЗПЕКА В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ
робоча програма навчальної дисципліни

Галузь знань **12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність **125 "КІБЕРБЕЗПЕКА"**
Освітній рівень **перший (бакалаврський)**
Освітня програма **"КІБЕРБЕЗПЕКА"**

Статус дисципліни
Мова викладання, навчання та оцінювання

обов'язкова
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.

Розробник:

Долгова Н.Г., к.т.н., доц. 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

Дисципліна “Безпека в інформаційно-комунікаційних системах” складається з двох модулів, в рамках першого розглядаються сучасні загрози мережевої безпеки, поняття забезпечення безпеки мережевих пристроїв, впровадження технологій брандмауера, впровадження системи запобігання вторгнень.

В рамках другого модуля дисципліни розглянуті питання забезпечення безпеки локальної мережі (LAN), криптографічні системи, впровадження віртуальних приватних мереж (VPN), впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA).

Мета навчальної дисципліни:

Метою дисципліни викладання навчальної дисципліни є навчання студентів принципам побудови комплексних систем захисту інформації для формування контуру безпеки бізнес-процесів в інформаційно-комунікаційних системах на основі Інтернет Технологій та застосунків.

Результатами вивчення даної дисципліни є придбання навичок з нейтралізації типових мережевих загроз, використання протоколу SNMP для захисту мережі, захисту від шкідливого програмного забезпечення та захист електронної пошти та веб-трафіку.

Характеристика навчальної дисципліни

Курс	3
Семестр	5
Кількість кредитів ECTS	6
Форма підсумкового контролю	екзамен

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Введення в мережі	Інформаційні системи та Інтернет технології
Математичні основи криптології	Основи технічного захисту інформації
Основи побудови та захисту сучасних операційних систем	Основи криптографічного захисту

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.	РН1 – 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	РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи

<p>та розуміння професії. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації</p>	<p>розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; 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. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації</p>	<p>РН 5 – адаптуватися в умовах частотої 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. 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 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>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні</p>	<p>РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та</p>

<p>та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.</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 кібератак, збоїв та відмов різних класів та походження.</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 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або</p>	<p>реагування на інциденти інформаційної та/або кібербезпеки;</p>
--	---

<p>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</p>	
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки</p>	<p>РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;</p>
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки 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</p>	<p>РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;</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.). 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 12 – розробляти моделі загроз та порушника</p>
<p>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КФ 2. Здатність до використання інформаційно-комунікаційних технологій,</p>	<p>РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та</p>

<p>сучасних методів і моделей інформаційної безпеки 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>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>протоколах передачі даних;</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 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 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або</p>	<p>РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;</p>

кібербезпеки.	
<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 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p>	<p>РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;</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 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 10. Здатність застосовувати методи та засоби криптографічного та технічного</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>захисту інформації на об'єктах інформаційної діяльності.</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 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 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/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>РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;</p>
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки 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,</p>	<p>РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;</p>

<p>інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p>	
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях. 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 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 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p>	<p>РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;</p>
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях. 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</p>	<p>РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;</p>

<p>процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем 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. 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.</p>	<p>РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах</p>
<p>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.</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>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 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;</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 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p>	<p>РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;</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 6. Здатність відновлювати штатне</p>	<p>РН 28 – 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;</p>

<p>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 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>КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</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 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p>	<p>РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;</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-</p>	<p>РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;</p>

<p>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>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 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 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;</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 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 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>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</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 і\або кібербезпеки;</p>

встановленою політикою інформаційної та/або кібербезпеки	
<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 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p>	<p>РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;</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 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p>	<p>РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації</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>КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з</p>	<p>РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;</p>

<p>встановленою політикою інформаційної та/або кібербезпеки</p>	
<p>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.</p>	<p>РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів;</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. 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</p>	<p>РН 44 – 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;</p>

<p>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>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 45 – застосовувати ріні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;</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</p>	<p>РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;</p>

<p>процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</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 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p>	<p>РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;</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 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 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або</p>	<p>РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;</p>

кібербезпеки.	
<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 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>РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;</p>
<p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</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 52 – використовувати інструментарій для моніторингу процесів 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>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.</p>	<p>РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз;</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 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>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 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ 2. Знання та розуміння предметної області та розуміння професії.</p> <p>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</p>	<p>РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні</p>

<p>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</p>	
--	--

Програма навчальної дисципліни

Змістовий модуль 1. Застосунки мережевої безпеки

- Тема 1. Сучасні загрози мережевої безпеки
- Тема 2. Забезпечення безпеки мережевих пристроїв
- Тема 3. Автентифікація, авторизація та облік
- Тема 4. Впровадження технологій брандмауера
- Тема 5. Впровадження системи запобігання вторгнень

Змістовий модуль 2. Мережева безпека

- Тема 6. Забезпечення безпеки локальної мережі (LAN)
- Тема 7. Криптографічні системи
- Тема 8. Впровадження віртуальних приватних мереж (VPN)
- Тема 9. Впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA)
- Тема 10. Знайомство з ASDM
- Тема 11. Управління безпечної мережею

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, презентації, бесіди, індивідуальні та групові міні-проекти.

Викладання дисципліни передбачає залучення пояснювально-ілюстративного (теми 1-11) репродуктивного (теми 3,4,5,6,8), дослідницького методів (теми 9,10), а також методів проблемного навчання (тема 11). Так під час проведення лекційних занять викладач надає здобувачам певний обсяг теоретичного матеріалу, з наданням пояснень у графічному вигляді (схеми, таблиці, презентації) та за допомогою прикладів розв'язання задач. На лабораторних заняттях здобувачі мають змогу отримати практичні навички розв'язання задач на підставі проблеми, сформульованої за тематикою заняття. Вдосконалення

практичних навичок відбувається під час виконання індивідуальних завдань та самостійної роботи.

Наведені методи навчання спрямовані на формування у здобувачів здатності розв'язання складних комплексних задач в галузі розробки веб-застосунків.

Порядок оцінювання результатів навчання

Програмою навчальної дисципліни передбачено лекційні, лабораторні та самостійні види робіт. Знання та компетентності, набуті студентами під час лекційних занять, оцінюються при написанні контрольних робіт та складанні тестів, навички, набуті під час лабораторних занять, оцінюються при розв'язанні задач, передбачених тематикою занять. Самостійна робота окремо не оцінюється, оскільки полягає у підготовці до інших видів занять і є невід'ємною складовою здобуття освіти. Оцінювання сформованих компетентностей здобувачів здійснюється за накопичувальною 100-бальною рейтинговою системою. Контрольні заходи включають

- поточний контроль, який здійснюється протягом семестру під час лекційних та лабораторних занять і оцінюється за сумою набраних балів (максимальна сума - 60 балів; мінімальна сума допуску до іспиту - 35 балів)

- модульний контроль передбачає виконання підсумкових контрольних завдань, які можуть включати творчу дослідницьку складову та потребують знань і вмінь, набутих під час вивчення комплексу матеріалу за темою модуля.

При поточному контролі знання здобувачів оцінюються за такими критеріями

- вільне володіння навчальним матеріалом в повному обсязі, з розумінням прикладів та можливістю наведення власних прикладів для пояснення суті матеріалу;

- демонстрація навичок застосування методів побудови математичних моделей для розв'язання прикладних задач;

- демонстрація навичок застосування інноваційних методів роботи під час розв'язування задач;

- демонстрація навичок пошуку та аналізу джерел інформації, обґрунтування отриманих результатів та формування висновків у роботі;

- демонстрація навичок роботи в команді при вирішенні комплексних завдань з розробки та аналізу математичних моделей.

Формування завдань та контроль їх виконання спрямовані на допомогу студентам у набутті навичок активного творчого мислення, прищеплення пізнавальних навичок і норм добросовісної співпраці. Основною вимогою до виконання завдань є самостійність їх виконання або визначення відсотка внеску за умов командної роботи.

Розподіл балів поточного оцінювання за видами робіт виглядає наступним чином.

Лекційні заняття: рівень оволодіння теоретичними знаннями визначається під час лекцій, за написання контрольних робіт та тестів (максимальна кількість балів становить – 20).

Лабораторні заняття: рівень набутих навичок застосування знань для розв'язання задач визначається правильністю виконання завдань лабораторних робіт (максимальна кількість балів становить 40).

Самостійна робота: рівень оволодіння навичками використання новітніх знань, методології та методів проведення наукових досліджень визначається за ступенем

підготовки аспіранта до виконання лабораторних робіт та написання контрольних робіт (в технологічній карті додаткових балів на цей вид робіт не передбачено).

Підсумковий контроль: проводиться з урахуванням екзамену.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування здобувачами компетентностей. Кожен екзаменаційний білет складається із 2 теоретичних питань та 1 практичного завдання, які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента та рівень його компетентності з навчальної дисципліни. Оцінювання кожного завдання екзаменаційного білету наступне: перше теоретичне питання оцінюється 10 балами; друге питання оцінюється 10 балами; третє практичне завдання – розрахункове, виконання його оцінюється 20 балами.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності". Здобувача слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімумально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімумально можлива кількість балів, набраних на екзамені, – 25. Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та 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

Т е м а	Форми та види навчання		Форми оцінювання	Мах бал
Т е м а 1 ·	<i>Аудиторна робота</i>			
	Лекція	Лекція №1. Сучасні загрози мережевої безпеки.	Робота на лекції	
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 2 ·	<i>Аудиторна робота</i>			
	Лекція	Лекція №2. Забезпечення безпеки мережевих пристроїв.	Робота на лекції	
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 3	<i>Аудиторна робота</i>			
	Лекція	Лекція №3. Автентифікація, авторизація та облік.		
	Лабораторне заняття	Лабораторна робота 1. Соціальна інженерія. Вивчення мережевих атак, а також інструменти для аудиту безпеки і проведення атак.	Захист лабораторної роботи	5
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Т е м а 4 ·	<i>Аудиторна робота</i>			
	Лекція	Лекція №4. Впровадження технологій брандмауера.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 2. Захист маршрутизатора для адміністративного доступу.		
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт.		

		Виконання лабораторних завдань		
Т е м а 5 .	Аудиторна робота			
	Лекція	Лекція №5. Впровадження системи запобігання вторгнень.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 2. Захист маршрутизатора для адміністративного доступу.	Захист лабораторної роботи	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
	Модульний контроль	Контрольна робота		10
Т е м а 6 .	Аудиторна робота			
	Лекція	Лекція №6. Забезпечення безпеки локальної мережі (LAN).	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 3. Захист адміністративного доступу за допомогою AAA і RADIUS.		
	Самостійна робота			
Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань			
Т е м а 7 .	Аудиторна робота			
	Лекція	Лекція №7. Криптографічні системи захисту інформації.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 3. Захист адміністративного доступу за допомогою AAA і RADIUS.	Захист лабораторної роботи	10
	Самостійна робота			
Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань			
Т е м а 8 .	Аудиторна робота			
	Лекція	Лекція №8. Впровадження віртуальних приватних мереж (VPN).	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 4. Налаштування зональних міжмережєвих екранів.		

	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Т е м а 9 ·	<i>Аудиторна робота</i>			
	Лекція	Лекція №9. Впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA).	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 4. Налаштування зональних міжмережевих екранів.	Захист лабораторної роботи	10
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Т е м а 10 ·	<i>Аудиторна робота</i>			
	Лекція	Лекція №10 " Знайомство з ASDM."	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 5. Налаштування системи запобігання вторгнень (IPS).		
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Т е м а 11 ·	<i>Аудиторна робота</i>			
	Лекція	Лекція №11. Управління безпечної мережею.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 5. Налаштування системи запобігання вторгнень (IPS).	Захист лабораторної роботи	10
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
	Модульний контроль	Контрольна робота		10
	Екзамен			40

Рекомендована література

Основна

1. Кібербезпека: сучасні технології захисту. Навчальний посібник для вищих навчальних закладів. / Остапов С.Е., Євсєєв С.П., Король О.Г. – Львів: «Новий світ-2000», 2019. – 678 с.
2. Технології захисту інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : навчальний посібник / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 213 с.
3. Інформаційна безпека держави: навчальний посібник / В. М. Рудницький, С. О. Гнатюк, Н. В. Лада, Р. В. Бреус. - Харків : ТОВ «ДІСА ПЛЮС», 2018. – 359 с.
4. ЗАКОН УКРАЇНИ Про захист інформації в інформаційно-комунікаційних системах <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

Додаткова

5. CCNA 200-301 Official Cert Guide Library By Wendell Odom, Published Dec 31, 2019 by Cisco Press. Part of the Official Cert Guide series <https://issuhub.com/view/index/33465>

Інформаційні ресурси в Інтернеті

6. EVE - віртуальне середовище в області мереж, безпеки та DevOps <https://www.eve-ng.net/>
7. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “Інженерія безпеки інформаційно-комунікаційних систем” <https://pns.hneu.edu.ua/course/view.php?id=8951>