

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

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)

Микола Афанасьєв
Микола АФАНАСЬЄВ

№02071211

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 *базова*
Мова викладання, навчання та оцінювання *українська*

Завідувач кафедри
кібербезпеки та
інформаційних технологій

СВ

Сергій ЄВСЕЄВ

Харків
2020

ЗАТВЕРДЖЕНО

на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробник:

Євсєєв С. П., д.т.н., проф. кафедри КІТ.

Корольов Р.В., к.т.н., доцент 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).

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	1
Кількість кредитів ECTS	5
Форма підсумкового контролю	екзамен

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Математичні основи криптології	Інформаційні системи та Інтернет технології

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КЗ 2. Знання та розуміння предметної області та розуміння професії.	РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; 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; 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; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; 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; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення 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

	<p>віддалених компонент; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; 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>КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</p>	<p>РН–10. виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН–11. виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН–13. аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–15. використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; 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; РН–18. використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН–19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–20. забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН–31. застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН–41. забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН–53. вирішувати задачі аналізу програмного коду на наявність можливих загроз.</p>
<p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p>	<p>РН-9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН-14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН-15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН-16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; 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; РН-18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН-20. Забезпечувати функціонування спеціального програмного</p>

	<p>забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;</p> <p>RH-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>RH-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> <p>RH-47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;</p> <p>RH-50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);</p> <p>RH-53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.</p>
<p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p>	<p>RH 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;</p> <p>RH 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>RH 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>RH 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>RH 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>RH 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;</p> <p>RH 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;</p> <p>RH 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;</p> <p>RH 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> <p>RH 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і\або кібербезпеки;</p> <p>RH 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів;</p> <p>RH 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>RH 45 – застосовувати рині класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;</p> <p>RH 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;</p> <p>RH 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз;</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>RH-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>RH-20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;</p> <p>RH-23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>RH-27 вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>RH-31 застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;</p> <p>RH-37 вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоків технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;</p> <p>RH-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>RH-48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;</p> <p>RH-49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;</p> <p>RH-52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;</p> <p>RH-53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.</p>
<p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p>	<p>RH-9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;</p> <p>RH-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>RH-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>RH-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>RH-28 аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-</p>

	<p>телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики 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>РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;</p> <p>РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;</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> <p>РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;</p> <p>РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів;</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>РН–45 застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;</p> <p>РН–46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.</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 багатofункціонального 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 проблемні лекції, презентації, бесіди, індивідуальні та групові проекти, майстер-класи.

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 дозволяє студенту скласти іспит, – 35 балів);

2) підсумковий/семестровий контроль, що проводиться у формі семестрового 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 критично осмислювати, вибирати та використовувати необхідний науковий, методичний і аналітичний інструментарій для управління в непередбачуваних умовах;

- вміння приймати, обґрунтовувати та забезпечувати реалізацію управлінських рішень в непередбачуваних умовах, враховуючи вимоги чинного законодавства, етичні міркування та соціальну відповідальність;

- вміння забезпечувати особистий професійний розвиток та планувати власний час.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Лекційні заняття: максимальна кількість балів становить 12 (робота на лекціях – 12).

Лабораторні заняття: максимальна кількість балів становить 48 (захист лабораторних робіт – 30, контрольні роботи – 18), а мінімальна – 24.

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

Підсумковий контроль: проводиться з урахуванням іспиту.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 3 практичних ситуацій (одне стереотипне, одне діагностичне та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни. Оцінювання кожного завдання екзаменаційного білету наступне: перше завдання – це 20 тестових завдань закритої форми, виконання його оцінюється 20 балами; друге завдання – присвячене розробленню структурної схеми побудови корпоративної мережі компанії, виконання його оцінюється 10 балами; третє завдання – розрахункове, виконання його оцінюється 10 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".

Студента 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.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

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

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D		
60 – 63	E	задовільно	не зараховано
35 – 59	FX	незадовільно	

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання	Форми оцінювання	Мак бал	
Тема 1	Аудиторна робота			
	Лекція	Проблемна лекція " Сучасні загрози мережевої безпеки "	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №1 "Соціальна інженерія. Вивчення мережевих атак, а також інструменти для аудиту безпеки і проведення атак "		
	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		
Тема 2	Аудиторна робота			
	Лекція	Лекція №2 " Забезпечення безпеки мережевих пристроїв "	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №1 "Соціальна інженерія. Вивчення мережевих атак, а також інструменти для аудиту безпеки і проведення атак "	Захист лабораторної роботи № 1	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		
М а	Аудиторна робота			

	Лекція	Лекція №3 " Автентифікація, авторизація та облік "	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №2 " Захист маршрутизатора для адміністративного доступу "		
	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		
Тема 4	Аудиторна робота			
	Лекція	Лекція №4. " Впровадження технологій брандмауера "	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №2 " Захист маршрутизатора для адміністративного доступу "	Захист лабораторної роботи № 2	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		
Тема 5	Аудиторна робота			
	Лекція	Лекція №5 " Впровадження системи запобігання вторгнень "	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №3 " Захист адміністративного доступу за допомогою AAA і RADIUS "	Контрольна робота №1	9
Тема 6	Аудиторна робота			
	Лекція	Лекція №6 "Забезпечення безпеки локальної мережі (LAN)"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №3 " Захист адміністративного доступу за допомогою AAA і RADIUS "	Захист лабораторної роботи № 3	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. Підготовка до екзамену		
М а	Аудиторна робота			

	Лекція	Лекція №7 "Криптографічні системи"	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №4. "Налаштування зональних міжмережєвих екранів "		
	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. Підготовка до екзамену		
Тема 8	Аудиторна робота			
	Лекція	Лекція №8 " Впровадження віртуальних приватних мереж (VPN)"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №4. "Налаштування зональних міжмережєвих екранів "	Захист лабораторної роботи № 4	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. Підготовка до екзамену		
Тема 9	Аудиторна робота			
	Лекція	Лекція №9 " Впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA)"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №5. "Налаштування системи запобігання вторгнень (IPS)"		
	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. Підготовка до екзамену		
Тема 10	Аудиторна робота			
	Лекція	Лекція " Знайомство з ASDM. "	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №5. "Налаштування системи запобігання вторгнень (IPS)"	Захист лабораторної роботи № 5	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. Підготовка до екзамену: виконання типових завдань за теорією		
Тема 11	<i>Аудиторна робота</i>			
	Лекція	Лекція " Управління безпечної мережею "	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №6. " Захист комутаторів 2-го рівня "		
	<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. Підготовка до екзамену: виконання типових завдань за практичною складовою		
	<i>Аудиторна робота</i>			
	Лабораторне заняття	Лабораторна робота №6. " Захист комутаторів 2-го рівня "	Захист лабораторної роботи № 6 Контрольна робота №2	14
<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. Підготовка до екзамену: виконання типових завдань за практичною складовою			

Рекомендована література

Основна

1. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсєєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С.Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6
2. С. П. Євсєєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.
3. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.
4. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.

Додаткова

5. Хорошко В. А. Методы и средства защиты информации. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с
6. Askoxylakis I., Ioannidis S., Katsikas S.K., Meadows C. (eds.) Computer Security - ESORICS 2016, Part I

Інформаційні ресурси в Інтернеті

7. <http://bezopasnost.biz>
8. <http://dstszi.gov.ua>
9. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “Безпека в інформаційно-комунікаційних системах” <https://pns.hneu.edu.ua/course/view.php?id=7087>.