Державний університет інтелектуальних технологій і зв'язку
Факультет Інформаційних технологій і кібербезпеки
Кафедра Кібербезпеки та технічного захисту інформації

"**ЗАТВЕРДЖУЮ**"

Ректор ДУІТЗ

_____ Олександр НАЗАРЕНКО

"____" _____ 2023 року

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Моніторинг та аудит інформаційно-комунікаційних систем
(шифр і назва навчальної дисципліни)

Рівень вищої освіти __другий (магістерський) рівень_____
Галузь знань __12 – Інформаційні технології_____
Спеціальність _125 – Кібербезпека та захист інформації
Спеціалізація (за наявності)_____
Освітня програма __Кібербезпека та захист інформації
Статус дисципліни __нормативна_____
Мова викладання __українська_____

Одеса 2023

Програма навчальної дисципліни Моніторинг та аудит інформаційно-комунікаційних систем для студентів освітнього рівня магістр за спеціальністю 125 – Кібербезпека та захист інформації

Розробник(и): викладач к.т.н., доц. Кільдішев Віталій Йосипович

Навчальна програма затверджена на засіданні кафедри Кібербезпеки та технічного захисту інформації

Протокол від "21" березня 2023 року № 8

Завідувач кафедри _____ В.В. Корчинський

(підпис) (ініціали та прізвище)

"21" березня 2023 року

Програму погоджено з гарантом освітньо-професійних програми магістрів

Гарант освітньо-професійної програми _____ В.В. Корчинський

(підпис) (ініціали та прізвище)

Програму погоджено з деканом факультету Інформаційних технологій і кібербезпеки

_____ Е.В. Василіу

(підпис) (ініціали та прізвище)

Програму схвалено навчально-методичною радою ДУІТЗ

Голова навчально-методичної ради ДУІТЗ,

Проректор з навчальної роботи _____ А.Г. Ложковський

(підпис) (ініціали та прізвище)

Протокол № ____ від _____ «____» _____ 2023 р.

ВСТУП

Програма вивчення нормативної навчальної дисципліни “Моніторинг та аудит інформаційно-комунікаційних систем” складена відповідно до освітньо-професійної програми підготовки магістрів галузі знань 12 “Інформаційні технології” за спеціальністю 125 “Кібербезпека та захист інформації”.

Дисципліна складається з 5 ECTS кредитів, викладається у семестрі 5.2.

Предметом вивчення навчальної дисципліни є автоматизовані системи моніторингу інформаційної безпеки та її основні складові, аудит безпеки інформаційних і комунікаційних систем, міждержавні та вітчизняні стандарти систем моніторингу інформаційної безпеки, аналіз ризиків для оцінки реальних загроз порушення інформаційної безпеки.

Міждисциплінарні зв’язки: *базується на професійно-орієнтованих дисциплінах.*

Основи програмування та бази даних (ОПБД);
Основи комп'ютерних технологій (ОКТ);
Основи телекомунікацій і комп'ютерні мережі (ОТКМ);
Архітектура та моделі безпеки (АМБ);
Забезпечення безпеки телекомунікацій (ЗБТ);
Безпека і експлуатація мережевих і хмарних технологій (БЕМХТ);
Проведення розслідування інцидентів інформаційної безпеки (ПРІІБ).

Програма навчальної дисципліни складається з такого змістовного модуля:

1. Моніторинг та аудит інформаційно-комунікаційних систем.

1. Мета та завдання навчальної дисципліни

1.1. Метою викладання навчальної дисципліни “Моніторинг та аудит інформаційно-комунікаційних систем” є формування основ знань щодо:

– аналізу, розробки і супроводження систем аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому (**РН14**);

– методів та технологій моніторингу та аудиту загроз для конфіденційності, цілісності та доступності інформації (**В5.31**);

– методів, засобів та інформаційних технологій виявлення несанкціонованого доступу до інформації на різних ієрархічних рівнях інформаційно-комунікаційної системи (**В5.32**);

– інструментарію (прикладні програми) моніторингу (аудиту) загроз для інформації в інформаційних системах та мережах (**В5.34**);

– інструментарію сканування та розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах (**В6.31**);

– способів сканування та розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах (**В6.З2**).

1.2. Основними завданнями вивчення дисципліни "Моніторинг та аудит інформаційно-комунікаційних систем" є формування наступних умінь та навичок:

– здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації (**В5.У1**);

– здійснювати моніторинг та аудит загроз для інформації, що озвучується (**В5.У2**);

– використовувати інструменти та технології безперервного моніторингу з метою оцінки ризиків, користуватися прикладними програмами моніторингу та аудиту загроз для інформації в інформаційних системах та мережах (**В5.У3**);

– проводити аудити/огляди систем і комплексів захисту інформації (систем безпеки інформації) та інформаційно-комунікаційних систем (**В5.У4**);

– проводити сканування вразливостей і розпізнання вразливостей в ІКС і системах безпеки (**В6.У1**).

У результаті вивчення навчальної дисципліни студент повинен отримати наступні **компетенції**:

Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому (**КФ9**).

Здатність здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію (доробку) систем і комплексів захисту інформації (**В5**).

Здатність проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки (**В6**).

2. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1. ***Моніторинг та аудит інформаційно-комунікаційних систем.***

1.1. *Загальні принципи аудиту інформаційної безпеки.*

Самостійно: Основні цілі та задачі моніторингу та аудиту інформаційних систем.

1.2. *Цілі та метод проведення зовнішнього аудиту.*

Самостійно: Основи проведення аудиту безпеки інформаційно-комунікаційних систем.

1.3. *Аналіз і оцінка ризиків інформаційної безпеки.*

Самостійно: Аналіз ризиків для оцінки реальних загроз порушення інформаційної безпеки.

1.4. *Безперервний внутрішній аудит інформаційної безпеки інформаційно-комунікаційних систем.*

Самостійно: Здійснення збирання та попередній аналіз даних, планування заходів з підготовки та проведення аудиту.

1.5. *Відповідність аудиту інформаційної безпеки міжнародним стандартам.*

Самостійно: Характеристика сучасної національної та міжнародної нормативної бази у сфері інформаційної безпеки.

1.6. *Тестування вразливостей. Етапи тестування на проникнення.*

Самостійно: Оформлення аудиторського звіту, аналіз відповідних ризиків та рекомендації щодо їх усунення.

3. Рекомендована література

ОСНОВНА

1. Тардаскіна Т. М. Менеджмент інформаційної безпеки в галузі зв'язку: [навч. посібник. Затверджено Міністерством освіти та науки України як посібник для вищих навчальних закладів. Лист № 1/11-7791 від 13 серпня 2010 року] / Т. М. Тардаскіна, В. Г. Кононович. – Одеса: ОНАЗ, 2010. – 268 с.

2. CISSP – Переклад книги Shon Harris "CISSP All-In-One Exam Guide". Електронний ресурс http://dorlov.blogspot.com/2011/05/issp-cissp-all-in-one-exam-guide.html

3. Програми та методики державної експертизи інформаційної захищеності телекомунікацій : навч. посіб. / С.М. Горохов, Н. В. Кондратьєва, В.Г. Кононович, С.В. Стайкуца; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 252 с.

ДОДАТКОВА

1. Кононович В.Г., Гладиш С.В. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 4: навч. посіб. – Одеса: ОНАЗ ім. О.С. Попова, 2009.

2. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ:ООО "Д.В.К.", 2004 . – 508 с.

Інформаційні ресурси

http://www.rangeforce.com/

4. Форма підсумкового контролю успішності навчання:

Іспит по закінченні вивчення дисципліни.

5. Засоби діагностики успішності навчання:

Відповіді на лабораторних заняттях, виконання та захист курсового проекту.