Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ О.О. Ілляшенко
(підпис) (ініціали та прізвище)

« 31 » серпня 2024 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Управління інформаційною безпекою
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2024 рік

Розробник: Карпенко А.С. старший викладач, Ph.D.
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол №1 від «30» 08 2024 р.

Завідувач кафедри д.т.н., професор _____ В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td rowspan="8">Кількість кредитів – 4(4.5)
Кількість модулів –2
Кількість змістових модулів – 4
Індивідуальне завдання не передбачено
Загальна кількість годин денна – 112 / 255
Кількість тижневих годин для денної форми навчання: аудиторних – 3(3) самостійної роботи студента – 4(4.5)</td><td rowspan="8">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 Кібербезпека
(код та найменування)

Освітня програма
"Безпека інформаційних та комунікаційних систем"
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td colspan="2">Обов’язкова</td></tr>
<tr><td colspan="2">Навчальний рік</td></tr>
<tr><td colspan="2">2024/ 2025</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>7-й</td><td>8-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>32 годин</td><td>32 годин</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>16 годин</td><td>32 годин</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>72 годин</td><td>71 годин</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td>залік</td><td>залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

Для денної форми навчання – 112/255.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: є отримання студентами необхідних знань та навиків для діяльності на основі застосування системи теоретичних знань і практичних навичок; формування комплексу засобів (правил, процедур, тощо) щодо управління

інформаційною безпекою; застосування комплексного підходу з забезпечення інформаційної безпеки в різних сферах діяльності (критичні системи та додатки).

Завдання: знати структуру нормативних актів та стандартів в сфері управління інформаційної безпекою; систему термінів та понять; організовувати основні процеси реалізації систем інформаційної безпеки (ІБ), а саме, планування, ризик-аналізу, вибору контрзаходів, тощо; вміти використовувати сучасні інформаційні технології при оцінювання ризиків критичної інфраструктури; визначати шляхи зниження ризиків, практично застосовувати методи забезпечення безпеки.

Мати уявлення: про методики розрахунку ризиків інформаційної безпеки на підприємствах.

Програмні компетентності. Дисципліна має допомогти сформувати у студентів такі компетентності:

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.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

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.

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 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання. В результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 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.

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН 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.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 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).

ПРН 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.

ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

ПРН 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.

ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

Міждисциплінарні зв’язки:

Пререквізити. Дисципліна базується на: «Нормативно-правове забезпечення інформаційної безпеки», «Комплексні системи захисту інформації: проектування, впровадження, супровід»

Кореквізити – «Дипломний робота (проект) бакалавра».

3. Програма навчальної дисципліни

Модуль 1
Змістовний модуль 1

ТЕМА 1. Вступ до навчальної дисципліни «Управління інформаційною безпекою»

Місце дисципліни в системі підготовки фахівця із організації інформаційної безпеки. Визначення головних понять пов'язаних з управлінням інформаційною безпекою. Історичні аспекти формування поняття управління інформаційною безпекою.

Предмет дисципліни, її цілі та задачі. Структура, завдання і форми контролю, основна література. Основні положення. Визначення області та межі дії систем управління інформаційною безпекою.

ТЕМА 2. Базові питання управління ІБ

Сутність та функції управління. Принципи, підходи та види управління. Цілі і завдання управління ІБ. Поняття системи управління. Поняття кіберінцидента / кібератаки.

ТЕМА 3. Область діяльності СУІБ

Поняття галузі діяльності СУІБ. Склад області діяльності (процеси, структурні підрозділи організації, кадри). Опис галузі діяльності (структура і зміст документа). Розслідування кіберінцидентів / кібератак. Розробка політик ІБ при забезпеченні бізнес-процесів. Дотримання політик ІБ при забезпеченні бізнес-процесів.

ТЕМА 4. Стандартизація в галузі управління ІБ

Стандартизація у сфері побудови систем управління. Існуючі стандарти та методології з управління ІБ: їх відмінності, сильні і слабкі сторони (на прикладі сімейства стандартів 1БО/IEC 2700х, СТО БР ІББС-1.0, ISO 17799, ISO 27001, КО/ШС 18044, СБ 25999 та ін).

ТЕМА 5. Серія стандартів ISO/IEC 27000. Історія серії стандартів ISO/IEC 27000

Історія серії стандартів ISO/IEC 27000. ISO/IEC 27002. Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою. ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво по застосуванню системи управління захисту інформації. ISO/IEC 27004 Інформаційні технології. Методи захисту. Вимірювання. ISO/IEC 27006 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою. Історія стандарту ISO/IEC 27001.

ТЕМА 6. Система управління ризиками на вимогу стандарту ISO/IEC 27001:2005. Додаток А стандарту ISO/IEC 27001:2005

Технології оцінки та аналізу ризиків. Попередній аналіз та оцінка інформаційних ресурсів організації. ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки. Реалізація вимог

стандарту. Засоби управління. Відповідальність керівництва. Методика впровадження системи управління інформаційною безпекою. Документація системи управління інформаційною безпекою.

ТЕМА 7. Системний підхід в управлінні системами менеджменту інформаційної безпеки. Інтеграція системи управління інформаційною безпекою та системи менеджменту якості

Модель PDCA. Додаток В стандарту ISO/IEC 27001:2005. Технологія керування системами менеджменту інформаційної безпеки. Оцінка рівня загроз та уразливостей. Методи вирішення багатокритеріальних завдань управління системами менеджменту інформаційною безпекою. Інтеграція системи менеджменту інформаційної безпеки за вимогами ISO/IEC 27001 та системи менеджменту якості за вимогами ISO 9001:2000. Додаток С стандарту ISO/IEC 27001.

Змістовний модуль №2

ТЕМА 8. Ризикологія ІБ

Основні визначення та положення ризикології. Мета процесу аналізу ризиків ІБ. Етапи та учасники процесу аналізу ризиків ІБ.

ТЕМА 9. Аналіз ризиків ІБ

Методики аналізу ризиків ІБ. Інвентаризація активів. Поняття активу. Типи активів. Джерела інформації про активи організації.

Визначення загроз ІБ і вразливостей для виділених на етапі інвентаризації активів. Оцінка ризиків ІБ. Планування заходів по обробці виявлених ризиків ІБ. Затвердження результатів аналізу ризиків ІБ у вищого керівництва. Використання результатів аналізу ризиків ІБ.

ТЕМА 10. Методика оцінки ризиків інформаційної безпеки компанії Digital Security

Метод оцінки ризиків на основі моделі загроз і вразливостей. Основні поняття та припущення моделі. Принцип роботи алгоритму. Вхідні дані: ресурси; критичність ресурсу; відділи, до яких належать ресурси; загрози, що діють на ресурси; уразливості, через які реалізуються загрози; ймовірність реалізації загрози через дану вразливість; критичність реалізації загрози через дану вразливість.

ТЕМА 11. Основні процеси СУІБ. Обов'язкова документація СУІБ

Процеси «Управління документами» та «Управління записами» (цілі і завдання процесів, вхідні/вихідні дані, ролі учасників, обов'язкові етапи процесів, зв'язку з іншими процесами СУІБ).

Процеси поліпшення СУІБ («Внутрішній аудит», «Коригувальні дії», «Запобіжні дії»). Процес «Моніторинг ефективності» (включаючи розробку показників ефективності). Поняття «Зрілість процесу». «Аналіз з боку вищого керівництва». Процес «Навчання і забезпечення обізнаності».

ТЕМА 12. Впровадження розроблених процесів. Документ «Положення про застосовність»

Етапи впровадження процесів та їх послідовність. Навчання співробітників, як один з етапів впровадження. Складності, які виникають при впровадженні процесів управління ІБ, і способи їх вирішення. Контроль над впровадженням процесів.

Документування процесу впровадження розроблених процесів. Типовий документ «Положення про застосовність». Мета документа. Структура і зміст документа. Процес розробки документа, рішення спірних ситуацій при розробці документа.

ТЕМА 13. Аудит систем управління інформаційною безпекою. Вимоги стандарту ISO 19011 до проведення аудитів.

Необхідність проведення аудиту систем управління інформаційною безпекою. Етапи внутрішнього аудиту систем управління інформаційною безпекою. Планування та підготовка, програма, тривалість і область діяльності аудиту систем управління інформаційною безпекою. Планування та підготовка аудиту систем управління інформаційною безпекою. Програма, тривалість і область діяльності аудиту систем управління інформаційною безпекою. Техніка аудиту. Алгоритм збору об'єктивних даних у процесі аудиту. Проведення коригувальних та попереджувальних дій. Вимоги до аудиторів. Етика аудиту. Рекомендації аудиторам.

ТЕМА 14. Сертифікація систем управління інформаційною безпекою. Проведення коригувальних та попереджувальних дій. Супровід систем управління інформаційною безпекою.

Організація сертифікаційного аудиту. Вибір організації для сертифікації. Організація перед сертифікаційного аудиту. Організація сертифікаційного аудиту. Консультаційні послуги з виконання коригувальних та попереджувальних дій щодо усунення зауважень, отриманих на перед сертифікаційного аудиті. Супровід систем управління інформаційною безпекою після сертифікаційного аудиту.

Модуль 2

Змістовний модуль №3

ТЕМА 15. **Аудит інформаційної безпеки**

Аудит інформаційної безпеки. Види аудиту. Основні складові системи аудиту інформаційної безпеки. Нормативне забезпечення аудиту інформаційної безпеки.

ТЕМА 16. **Внутрішній аудит СМІБ за вимогами ISO/IEC 27001 та ISO 19011**

Загальна характеристика внутрішніх аудитів СМІБ**.** Розробка програми внутрішнього аудиту на рік. Розробка плану аудиту протягом року. Розробка анкет відповідно до критеріїв аудиту. Підготовка до проведення аудиту на місці. Розробка звіту про аудит. Розробка корегувальних та запобіжних заходів. Перевірка виконання заходів і аналіз результативності. Підготовка звіту для вищого керівництва.

ТЕМА 17. **Комплексний аудит інформаційної безпеки**

Основні етапи аудиту безпеки інформаційних систем. Постановка задачі та уточнення обсягу робіт. Збір і аналіз інформації. Проведення аналізу ризиків.

Розробка рекомендацій. Оцінка діяльності з управління інформаційною безпекою організації. Основні положення стандарту ISO/IEC 27004:2009. Вимірювання, показники і метрика безпеки.

ТЕМА 18. **Управління інцідентами інформаційної безпеки.**

Базові принципи, терміни та визначення. Цілі управління інцидентами. Стандарти, рекомендації та найкращі світові практики щодо управління інцидентами інформаційної безпеки. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035. Особливості менеджменту інцидентів відповідно до ITIL. Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки.

Змістовний модуль №4

ТЕМА 19. Огляд стандарту **ISO/IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги»**

Приклади вразливостей, які можуть бути використані для реалізації відповідних загроз для комерційної структури. Ідентифікація активів підприємства для оцінки ризиків.

ТЕМА 20. **Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT**

Загальна характеристика діяльності груп CERT/CSIRT. Етапи створення груп CERT/CSIRT. Класифікація груп CERT/CSIRT за галузевою ознакою. Склад команд CERT/CSIRT. Сервіси, що надаються групами реагування на інциденти. Обробка інцидентів інформаційної безпеки групами CERT/CSIRT. Документаційне забезпечення процесу управління інцидентами інформаційної безпеки.

ТЕМА 21. **Політика безпеки інформації**

Методичні підходи до розробки політики інформаційної безпеки підприємства. Порядок розробки політики та етапи.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с.р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1. *Базові питання управління інформаційною безпекою та стандарти*					
Тема 1. Вступ до навчальної дисципліни «Управління інформаційною безпекою»	9	4			5
Тема 2. Базові питання управління ІБ	9	2		2	5
Тема 3. Область діяльності СУІБ	9	2		2	5

1	2	3	4	5	6
Тема 4. Стандартизація в галузі управління ІБ	9	2		2	5
Тема 5. Серія стандартів ISO/IEC 27000. Історія серії стандартів ISO/IEC 27000.	9	2		2	5
Тема 6. Система управління ризиками на вимогу стандарту ISO/IEC 27001:2005. Додаток А стандарту ISO/IEC 27001:2005.	7	2			5
Тема 7. Системний підхід в управлінні системами менеджменту інформаційної безпеки. Інтеграція системи управління інформаційною безпекою та системи менеджменту якості.	7	2			5
Разом за змістовим модулем 1	59	16	0	8	35
Змістовий модуль 2. *Аналіз і оцінка ризиків. Впровадження сертифікація та аудит СУІБ*					
Тема 8. Ризикологія ІБ	6	2			4
Тема 9. Аналіз ризиків ІБ	9	2		2	5
Тема 10. Методика оцінки ризиків інформаційної безпеки компанії Digital Security	11	4		2	5
Індивідуальне завдання	7				7
Тема 11. Основні процеси СУІБ. Обов'язкова документація СУІБ	9	2		2	5
Тема 12. Впровадження розроблених процесів. Документ «Положення про застосовність»	7	2		2	3
Тема 13. Аудит систем управління інформаційною безпекою. Вимоги стандарту ISO 19011:2002 до проведення аудитів	5	2			3
Тема 14. Сертифікація систем управління інформаційною безпекою. Проведення коригувальних та попереджувальних дій. Супровід систем управління інформаційною безпекою.	7	2			5
Разом за змістовим модулем 2	61	16	0	8	37
Разом за модулем 1	120	32		16	72
Модуль 2					
Змістовий модуль 3. *Аудит та управління інцидентами інформаційної безпеки.*					
Тема 15. Аудит інформаційної безпеки.	18	4		4	10
Тема 16. Внутрішній аудит СМІБ за вимогами ISO/IEC 27001 та ISO 19011.	18	4		4	10

1	2	3	4	5	6
Тема 17. Комплексний аудит інформаційної безпеки.	18	4		4	10
Тема 18. Управління інцидентами інформаційної безпеки.	20	4		6	10
Разом за змістовим модулем 3	74	16	0	18	40
Змістовий модуль 4. *Реагування на інциденти та політика інформаційної безпеки.*					
Тема 19. Огляд стандарту ISO/IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги».	23	6		6	11
Тема 20. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.	20	6		4	10
Тема 21. Політика безпеки інформації.	18	4		4	10
Разом за змістовим модулем 4	61	16	0	14	31
Разом за модулем 2	135	32		32	71
Усього за дисципліну	255	64		48	143

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
...	*Не передбачено*	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	2	3
	Не передбачено	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Дослідження можливості оцінки надійності паролів користувачів систем управління ІБ.	2
2	Дослідження можливості управління функціями ІБ через реєстр.	2

3	Дослідження можливості реалізації програмних методів гарантованого знищення даних з HDD.	2
4	Дослідження можливості реалізації програмних методів відновлення даних з HDD.	2
5	Дослідження можливості оцінки можливості підбору паролю до систем управління ІБ.	2
6	Дослідження можливості реалізації програмних методів відновлення даних з SSD.	2
7	Дослідження та реалізація методики аналізу ризиків корпорації Microsoft.	2
8	Закріплення матеріалу лекції щодо аудиту інформаційної безпеки.	2
9	Отримання практичних навичок з розроблення документів. Опитувальник, бланк для фіксації результатів внутрішнього аудиту, протокол відхилень.	4
10	Закріплення матеріалу лекції щодо комплексного аудиту інформаційної безпеки	4
11	Отримання практичних навичок з аналізу СМІБ	4
12	Отримання практичних навичок з виявлення вразливостей, які можуть бути використані для реалізації відповідних загроз для комерційної структури.	6
13	Закріплення матеріалу лекції щодо функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT	6
14	Отримання практичних навичок аналізу політик інформаційної безпеки	4
	Разом	**48**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Опрацювати: Міжнародний стандарт ISO/IEC 27000:2018 Information technology Security techniques. Information security management systems. Overview and vocabulary.	10
2	Опрацювати: Міжнародний стандарт ISO/IEC 27002:2013 Information technology Security techniques. Code of practice for information security controls.	14
3	Ознайомитись з методиками оцінки ризиків, що використовуються на підприємствах України.	15
4	Опрацювати: Методика оцінки ризиків інформаційної безпеки компанії Digital Security на основі інформаційних потоків.	10
5	Опрацювати: стандарт ISO 19011:2002 до проведення аудитів.	10
6	Ознайомитись з міжнародними стандартами серії BSI 17999	6

7	Індивідуальне завдання	7
8	Опрацювання стандарту CobiT	10
9	Опрацювання стандарту ITIL	10
10	Опрацювання стандарту ISO/IEC 15408	10
11	Опрацювання стандарту ISO/IEC 270001	12
12	Кращі світові практики політик інформаційної безпеки	10
13	Опрацювання стандарту CobiT	10
14	Опрацювання стандарту ITIL	9
	Разом	**72**

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
1	Побудова моделі інформаційних потоків, моделі загроз та оцінка ризиків на підприємстві.	7

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, модульного контролю (тести за кожною темою), підсумковий контроль у вигляді іспиту.

12. Розподіл балів, які отримують студенти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1			
Робота на лекціях	0…1	16	0…16
Виконання і захист лабораторних робіт	0...5	8	0...40
Модульний контроль	0…22	2	0…44
Усього за семестр			**0 …100**
Модуль 2			
Робота на лекціях	0…1	16	0…16

Виконання і захист лабораторних робіт	0...5	8	0...40
Модульний контроль	0…22	2	0…44
Усього за семестр			**0…100**

Лабораторна робота має бути здана протягом двох тижнів. Для отримання максимальної оцінки повіни здати протягом трьох днів з моменту виконання за розкладом занять; 4 – 6; 3 – 9; 2 – 12; 1-14 днів

Участь у конференції -10 балів.

Стаття у фаховому журналі -20 балів

Критерії оцінювання знань студента під час іспиту

Задовільно (60-74). Захистити не менше 85% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення робіт щодо розвитку та підтримки функціонування СТЗІ.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 95% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації та проведення робіт щодо розвитку та підтримки функціонування СТЗІ. Мати необхідний обсяг умінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та вміти їх застосовувати. Уміти виконувати інформаційне забезпечення СТЗІ.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=1611, на якому розміщено навчально-методичний комплекс дисципліни, який включає в себе:

– робоча програма дисципліни;

– конспект лекцій (презентації), в тому числі в електронному вигляді, який за змістом повністю відповідає робочій програмі дисципліни;

– журнал успішності.
– Посилання на практики

14. Рекомендована література

1. Домарєв В. В., Швець В. А., Шестакова В. В. Організаційне забезпечення захисту інформації з обмеженим доступом: Навчальний посібник. / Національний авіаційний університет; МОН. – К.: НАУ, 2006. – 108 с.
2. Основи управління інформаційною безпекою: навч. посібник /А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.
3. Управління інформаційною безпекою. Конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1,11 Мбайт). – Київ:КПІ ім. Ігоря Сікорського, 2021. – 258 с.
4. Управління інформаційною безпекою: навчально-методичний посібник./ А. І. Поворознюк, О.А. Поворознюк – Харків: НТУ «ХПІ», 2021. – 135 с.
5. Управління інформаційною безпекою. Конспект лекцій: навчальний посібник для студентів спеціальності 125 «Кібербезпека» / С. О. Носок, О. М. Фаль, В. М. Ткач. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.
6. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навчальний посібник. / МОН. – К.: Кондор, 2008. – 383 с.
7. Mastering Information Security Compliance Management: A comprehensive handbook on ISO/IEC 27001: 2022 compliance.
8. Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement Hardcover – Illustrated, March 30 2009 by W. Krag Brotby CISM.

Стандарти

1. Міжнародний стандарт ISO 27001 ISO/IEC 27001 Information technology Security techniques. Information security management systems. Requirements.
2. Міжнародний стандарт ISO/IEC 27000 Information technology Security techniques. Information security management systems. Overview and vocabulary.
3. Міжнародний стандарт ISO/IEC 27002 Information technology Security techniques. Code of practice for information security controls.

15. Інформаційні ресурси

1. Державна служба спеціального зв'язку та захисту інформації України [Электрон. ресурс]. - Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/index
2. Міжнародна організація зі стандартизації [Электрон. ресурс]. - Режим доступу: https://www.iso.org/isoiec-27001-information-security.html