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

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

ЗАТВЕРДЖУЮ

Керівник проектної групи
_____ В.С. Харченко
(підпис) (ініціали та прізвище)
«_30_» __серпня_ 2019 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Комплексні системи захисту інформації: проектування, впровадження, супровід
(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 2019 рік

Робоча програма Комплексні системи захисту інформації: проектування, провадження, супровід
(назва дисципліни)
для студентів за спеціальністю 125 "Кібербезпека"
освітньою програмою Безпека інформаційних і комунікаційних систем

«26» 08 2019 р., – 17 с.

Розробник: Пєвнєв В.Я., доцент кафедри 503, к.т.н., доцент _____
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Цуранов М.В., ст. викладач кафедри 503 _____
(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 2019 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, напрям підготовки, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 12.0</td><td rowspan="9">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних і комунікаційних систем
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Цикл загально-професійної підготовки</td></tr>
<tr><td>Кількість модулів – 3</td><td rowspan="2">Навчальний рік
2019/2020</td></tr>
<tr><td>Кількість змістових модулів – 5</td></tr>
<tr><td>Індивідуальне завдання: Курсовий проект</td><td rowspan="2">Семестр: 7-й, 8-й</td></tr>
<tr><td>Загальна кількість годин – 124/360</td></tr>
<tr><td rowspan="5">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 4,5</td><td>Лекції [1)]56 год.</td></tr>
<tr><td>Практичні, семінарські
12 год.</td></tr>
<tr><td>Лабораторні[1)]
56 год.</td></tr>
<tr><td>Самостійна робота
236 год.</td></tr>
<tr><td>Індивідуальні завдання: Курсовий проект</td></tr>
<tr><td></td><td>Вид контролю: модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

Для денної форми навчання – 124/360.

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

2. Мета та завдання навчальної дисципліни

Мета (ОК30, ВБ 1.7, ВБ 1.15): діяльності на основі застосування системи теоретичних знань і практичних навичок з виявлення способів порушення інформаційної безпеки при роботі комп'ютерних систем обробки інформації; вирішення задач захисту програм та даних програмно-апаратними засобами; застосування системного підходу до забезпечення інформаційної безпеки, включаючи комплекс організаційних заходів..

Завдання (ОК30, ВБ 1.7, ВБ 1.15): застосовувати знання до вирішення задач інформаційної безпеки; обирати потрібні організаційні та інженерно-технічні заходи, засоби і методи захисту інформації; аналізувати вхідні данні та обирати методи оцінки якості систем та моделей.

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.
- 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 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
- 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 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
- 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 6 критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
- 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 10 виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
- ПРН 11 виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;
- ПРН 12 розробляти моделі загроз та порушника;
- ПРН 13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
- ПРН 14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
- ПРН 15 використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
- ПРН 16 реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
- ПРН 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;

- ПРН 18 використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
- ПРН 19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
- 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 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;
- ПРН 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;
- ПРН 30 здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
- ПРН 31 застосовувати теорії та методи захисту для забезпечення безпеки 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 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;
- ПРН 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;

- ПРН 36 виявляти небезпечні сигнали технічних засобів;
- ПРН 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;
- ПРН 38 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
- ПРН 39 проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
- ПРН 40 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
- 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 ріні 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 47 вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
- ПРН 48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
- ПРН 49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
- ПРН 50 забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);

- ПРН 53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.

В результаті засвоєння курсу “Комплексні системи захисту інформації: проектування, впровадження, супровід” студент повинен

знати:

1. Загальні аспекти проблематики в галузі інформаційної безпеки (сучасний стан задач та проблем, загрози та види руйнівних програм та атаки на інформаційні та комунікаційні системи, вимоги до їх захищеності).

2. Встановлену політику інформаційної та/або кібербезпеки.

3. Методи функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

4. Методи забезпечування захисту інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки..

5. Характеристику методів реалізації основних функцій системи захисту інформації.

6. Принципи відновлювання штатного функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

вміти:

1. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-комунікаційних системах

2. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

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

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

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

6. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-комунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

7. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.

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

мати уявлення:

про можливості реалізації перспективних систем інформаційної та/або кібербезпеки та методів використання програмних і програмно-апаратні комплекси захисту інформаційних ресурсів, що використовують нові принципи.

Міждисциплінарні зв'язки. Дисципліна базується на знаннях, отриманих під час вивчення дисциплін: «Прикладна криптологія», «Курс на вибір 1 Захист інформації в інформаційно-комунікаційних системах», «Надійність та функціональна безпека інформаційно-управляючих систем», «Системи технічного захисту інформації», «Нормативно-правове забезпечення інформаційної безпеки», «Курс на вибір 1 Технології захисту інформації», «Курс на вибір 2 (КП) Технології захисту інформації», «Організація баз даних», «Мікропроцесорні системи», «Web-технології», «Курс на вибір 3 Захист інформації в інформаційно-комунікаційних системах», «Управління інформаційною безпекою», «Мікропроцесорні системи захисту інформації», «Курс на вибір 3 Технології захисту інформації», «Мікропроцесорні системи захисту інформації (КП)», «Технології програмування (КП)».

Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для дисциплін: "Дипломний робота (проект) бакалавра", "Мікропроцесорні системи захисту інформації", "Мікропроцесорні системи", "Промислові контролери".

3. Програма навчальної дисципліни

Модуль 1.

Змістовний модуль 1.

ТЕМА 1. Захист програм та даних

Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі. Вимоги до знань та вмінь тих, хто навчається. Характеристика рекомендованих під час вивчення дисципліни джерел інформації. Характеристика сучасного стану проблематики в галузі забезпечення захисту інформації в інформаційних і комунікаційних системах та мережах.

Руйнуючі програмні засоби (РПЗ). Типи РПЗ. Тенденції розвитку РПЗ. Методи захисту від РПЗ. Недоліки існуючих засобів захисту від РПЗ

Типи шкідливого ПЗ. Класифікація шкідливих програм. Принципи створення та аналізу троянських програм. Життєвий цикл вірусу. Принципи створення та аналізу вірусів.

Протидія і виявлення троянських програм, черв'яків та вірусів. Основи роботи антивірусних программ. Сигнатурний аналіз. Евристичні аналізатори. Поведінкові блокатори. Протидія шкідливому коду. Шкідливе ПЗ для мобільних пристроїв.

Захист програмного забезпечення. Ідентифікація програм та захист авторських прав

Тема 2. Захист в комплексних системах.

Механізми захисту комплексних систем Підсистема безпеки операційної системи та виконувані нею функції. Реалізація підсистем безпеки у найбільш розповсюджених операційних системах. Критерії захищеності операційних систем

Операційна система iOS. Операційна система Android. Операційна система Windows Phone. Операційна система BlackBerry.

Організація контролю доступу в ОС. Руткіти та шпигунські програми. Інструменти, що використовуються для здійснення атак на операційні системи. Атака на парольний захист. Протидія атакам на операційні системи

Переповнення буферу. Поняття стеку та купи. Функції стеку викликів. Сегментація пам'яті. Причини виникнення переповнення буферу. Захист від переповнення буферу. Запобігання виконання даних

Змістовний модуль 2.

Тема 3. Захист в мережах

Методи та засоби реалізації загроз в комп'ютерних системах та мережах. Загальні поняття (загроза, вразливість, атака, несанкціонована дія, порушник). Класифікація порушників і типів засобів реалізації загроз. Класифікація загроз безпеки інформації, що передається по мережі. Класифікація способів порушення автентичності суб'єктів та даних. Потенційні можливості порушення захищеності даних, що передаються по інформаційних каналах.

Засоби забезпечення безпеки в обчислювальних мережах. Захист серверів та робочих станцій. Засоби захисту локальних мереж при приєднанні до Інтернету. Технологія міжмережних екранів Технологія віртуальних приватних мереж. Методи та засоби захисту мобільного програмного забезпечення

Безпека веб-серверів та веб-застосувань. Вразливості веб-серверів та веб-застосувань. Види атак на веб-сервер. Види атак на веб-застосування. Механізми захисту веб-серверів та веб-застосувань. ПЗ для сканування веб-серверів та веб-застосувань на вразливості. Тестування на вразливість до атак. Методика оцінки вразливостей. Тестування на вразливості. Сканери вразливостей. Послідовність дій при виконанні тестування веб-серверів та веб-застосувань на вразливість до атак згідно з OWASP.

Механізми DoS/DDoS атак. Об'єкти та види DoS атак. Захист від DoS/DDos атак.

Безпека в безпровідних мережах. Збір інформації про безпровідні мережі. Шифрування та автентифікація в безпровідних мережах. Атака на безпровідні мережі. Засоби захисту від безпровідних атак. Bluetooth

Модуль 2.

Змістовний модуль 3.

Тема 4. ***Захист в системах передачі даних та системах зв'язку***

Методи та технології захисту інформації в системах передачі даних та системах зв'язку. Засоби захисту захист інформації в системах передачі даних та системах зв'язку. Організаційні засади забезпечення захисту інформації

Типи атак на систему передачі даних. Механізми захисту від атак. Отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел. Способи протидії пасивному збору інформації. Засоби активного сбору інформації про систему передачі даних. Пошук вразливостей та інструменти сканування вузлів систем передачі даних та систем зв'язку на вразливості. Оцінка захищеності інформації в системах передачі даних та системах зв'язку.

Механізми захисту від збору інформації, сканування та проникнення. Системи виявлення вторгнень та системи запобігання вторгненням.

Змістовний модуль 4.

Тема 5. ***Загальні відомості***

Місце стеганографічних систем у сфері кібербезпеки. Терміни та визначення. Принципи побудови стеганографії. Структурна схема та математична модель типової стегосистеми. Протоколи. Методи приховування інформації. Класифікація методів стеганографії. Класична стеганографія. Комп'ютерна стеганографія. Цифрова стеганографія. Мережева стеганографія. Цифрові водяні знаки

Тема 6. ***Використання стеганографічних систем***

Технологічна схема захисту. Приховування інформації в тексті. Методи довільного інтервалу. Синтаксичні та семантичні методи. Приховування даних в нерухомих зображеннях. Приховування даних в просторової області. Метод заміни найменш значущого біта. Метод псевдовипадкового інтервалу. Метод блокового приховування. метод квантування зображення. Приховування даних в частотної області зображення. Метод Коха і Жао. Метод Хсу і Ву. Метод Фрідріх. Методи розширення спектру. Статистичні методи. Структурні методи. Приховування даних в ауді сигналах. Кодування найменш значущих біт. Метод фазового кодування. Метод розширення спектра. Приховування даних з використанням луна - сигналу.

Модуль 3.

Змістовний модуль 5.

Побудова захищеної мережі відеоспостереження. Побудова схеми контрольованої зони. Вибір камер відеоспостереження.

4. Структура навчальної дисципліни

Назви змістовних модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с.р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. *Базові питання управління інформаційною безпекою*					
Тема 1. Захист програм та даних	**26**	**8**		**8**	**10**
Тема 2. Захист в операційних системах	**29**	**8**		**8**	**13**
Разом за змістовним модулем 1	**55**	**16**		**16**	**23**
Змістовний модуль 2. *Стандарти в галузі управління інформаційною безпекою*					
Тема 3 Захист в мережах	**42**	**16**		**16**	**10**
Разом за змістовним модулем 2	**42**	**16**		**16**	**10**
Усього годин	**120**	**32**		**32**	**56**
Модуль 2					
Змістовний модуль 3. *Аналіз і оцінка ризиків*					
Тема 4. Захист в системах передачі даних та	**56**	**12**		**12**	**32**

1	2	3	4	5	6
системах зв'язку.					
Разом за змістовним модулем 3	**56**	**12**		**12**	**32**
Змістовний модуль 4. *Впровадження сертифікація та аудит СУІБ*					
Тема 5 Загальні відомості	**62**	**6**		**6**	**50**
Тема 6 Використання стегонографічних систем	**62**	**6**		**6**	**50**
Разом за змістовним модулем 4	**124**	**12**		**12**	**100**
Усього годин	**180**	**24**		**24**	**132**
Модуль 3					
Змістовний модуль 5. *Побудова захищеної системи відеоспостереження*	**60**		**12**		**48**
Усього годин	**60**		**12**		**48**
Усього за дисципліну	**360**	**56**	**12**	**56**	**236**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	*Не передбачено*	
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	*Курсове проектування*	12
	Разом	12

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Дослідження можливості виявлення вірусної активності вбудованими засобами ОС.	4
2	Дослідження можливості використання описаних вразливостей для вбудовування в вірусний код	4
3	Дослідження можливостей використання Metasploit для створення та відлагодження експлойтів.	4
4	Дослідження ефективності атак на парольний захист	4

5	Дослідження атаки типа «переповнення буферу» та методів протидії.	4
6	Дослідження методів пасивного та активного збору інформації про мережу.	4
7	Дослідження механізмів захисту мережі від збору інформації, сканування та проникнення	4
8	Дослідження алгоритмів завадостійкого кодування	4
9	Дослідження методів м'якого кодування	4
10	Порівняльний аналіз методів завадостійкого кодування	4
11	Дослідження цифрового водяного знаку	4
12	Дослідження можливостей розміщення повідомлення у текстовому файлі	4
13	Дослідження можливостей розміщення повідомлення у графічному файлі	4
14	Дослідження можливостей розміщення повідомлення у аудіо файлі	4
	Разом	56

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Руйнуючі програмні засоби (РПЗ). Типи РПЗ. Тенденції розвитку РПЗ. Методи захисту від РПЗ. Недоліки існуючих засобів захисту від РПЗ Типи шкідливого ПЗ. Класифікація шкідливих програм. Принципи створення та аналізу троянських програм. Життєвий цикл вірусу. Принципи створення та аналізу вірусів	15
2	Організація контролю доступу в ОС. Руткіти та шпигунські програми. Інструменти, що використовуються для здійснення атак на операційні системи. Атака на парольний захист. Протидія атакам на операційні системи	22
3	Безпека веб-серверів та веб-застосувань. Вразливості веб-серверів та веб-застосувань. Види атак на веб-сервер. Види атак на веб-застосування. Механізми захисту веб-серверів та веб-застосувань. ПЗ для сканування веб-серверів та веб-застосувань на вразливості. Тестування на вразливість до атак. Методика оцінки вразливостей. Тестування на вразливості. Сканери вразливостей. Послідовність дій при виконанні тестування веб-серверів та веб-застосувань на вразливість до атак згідно з OWASP.	30
4	Типи атак на систему передачі даних. Механізми	25

	захисту від атак. Отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел. Способи протидії пасивному збору інформації. Засоби активного сбору інформації про систему передачі даних. Пошук вразливостей та інструменти сканування вузлів систем передачі даних та систем зв'язку на вразливості. Оцінка захищеності інформації в системах передачі даних та системах зв'язку..	
5	Класіфікація методів стеганографії. Класична стеганографія. Комп'ютерна стеганографія. Цифрова стеганографія. Мережева стеганографія. Цифрові водяні знаки	20
6	Статистичні методи. Структурні методи. Приховування даних в аудісігналах.Кодіроване найменш значущих біт. Метод фазового кодування. Метод розширення спектра. Приховування даних з використанням луна - сигналу.	34
	Разом	**146**

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	*Курсовий проект*	12

10. Методи навчання

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

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
модуль 1			
Лекції	0…1	16	0…16
Лабораторні роботи	0...4	8	0…32
Модульний контроль	0…50	1	0…50
Індивідуальне завдання	0…2	1	0…2
Усього за семестр 7			**0…100**
модуль 2			
Лекції	0…1	12	0…12
Лабораторні роботи	0…6	6	0…36
Модульний контроль	0…50	1	0…50
Індивідуальне завдання	0…2	1	0…2
Усього за семестр 8			**0…100**
модуль 3			
Індивідуальне завдання (курсовий проект)	0…100	1	0…100
Усього за семестр 8			**0…100**

12.2. Якісні критерії оцінювання

В результаті засвоєння курсу студенти повинні:

вміти:

1. самостійно управляти ризиками на вимогу стандарту ISO/IEC 27001:2005;
2. самостійно будувати систему управління інформаційною безпекою;
3. самостійно оцінити надійність систем управління інформаційною безпекою;
4. самостійно проводити аудит систем управління інформаційною безпекою.

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

12.3. Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 75% від усіх завдань лабораторних занять.

Добре (75-89). Твердо знати мінімум, захистити не менше 90% завдань лабораторних занять.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати.

Розподіл балів, які отримують студенти за виконання курсового проекту

Пояснювальна записка	Ілюстративна частина	Захист роботи	Сума
до **40**	до **20**	до **40**	**100**

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

1. Презентації лекцій.
2. Керівництво до лабораторних робіт.

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. Сердюк В.А. Организация и технология защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В. А. Сердюк ; Государственный универ¬ситет - Высшая школа экономики .— Москва : ГУ ВШЭ, 2011 .— 573 с.
3. Анисимов А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов ; Интернет-университет информациионных технологий .— Москва : ИНТУИТ : БИНОМ. Лаб. знаний, 2010 .— 175 с.
4. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навчальний посібник. / МОН. – К.: Кондор, 2008. – 383 с.

Стандарти

1. Міжнародний стандарт ISO 27001 ISO/IEC 27001:2013 Information technology Security techniques. Information security management systems. Requirements.
2. Міжнародний стандарт ISO/IEC 27000:2018 Information technology Security techniques. Information security management systems. Overview and vocabulary.
3. Міжнародний стандарт ISO/IEC 27002:2013 Information technology Security techniques. Code of practice for information security controls.

15. Інформаційні ресурси

1. http://www.solon-press/ ru
2. http://bookash.pro/ru/s/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B5+%D0%B2%D0%B8%D1%80%D1%83%D1%81%D1%8B/
3. Державна служба спеціального зв'язку та захисту інформації України [Электрон. ресурс]. Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/index
4. Міжнародна організація зі стандартизації [Электрон. ресурс]. Режим доступу: https://www.iso.org/isoiec-27001-information-security.html