ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Управління проектами, інформаційних технологій та телекомунікацій
(назва кафедри)

ЗАТВЕРДЖУЮ
Голова Вченої ради ННІЦЗ
_____А.Г.Ренкас
(підпис) (прізвище та ініціали)

"_____" _____ 201__ р

БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

ПРОГРАМА

навчальної _____нормативної_____дисципліни
(нормативної, вибіркової)

підготовки _____магістра_____
(назва освітнього ступеня)

Спеціальності 122 «Комп'ютерні науки та інформаційні технології»
(шифр і назва спеціальності)

Львів
2016 рік

Розробники програми: Бурак Н.Є., викладач кафедри управління проектами, інформаційних технологій та телекомунікацій, кандидат технічних наук

Рецензент: Мандрона М.М., старший викладач кафедри управління інформаційною безпекою, кандидат технічних наук

Програму рекомендовано кафедрою управління проектами, інформаційних технологій та телекомунікацій

Протокол від "31" серпня 2016 року № 1

Завідувач кафедри управління проектами,
інформаційних технологій
та телекомунікацій
д.т.н, професор _____ (__Мартин Є.В.__)
(підпис) (прізвище та ініціали)

Схвалено Вченою радою навчально-наукового інституту цивільного захисту

Протокол від "____" _____ 201__ року № ____

ВСТУП

Програма вивчення *нормативної* навчальної дисципліни «Безпека інформаційно-комунікаційних систем» складена відповідно до освітньої програми підготовки *магістра* спеціальності 122 «Комп'ютерні науки та інформаційні технології».

Предметом вивчення навчальної дисципліни є сучасні методи захисту інформації в інформаційно-комунікаційних системах, особливості забезпечення безпеки у розподілених системах, апаратні та програмні складові систем захисту.

Міждисциплінарні зв'язки: навчальна дисципліна «Безпека інформаційно-комунікаційних систем» належить до циклу дисциплін професійної підготовки та нерозривно пов'язана із такими професійно-орієнтованими курсами, як «Телекомунікаційні системи та мережі», «Спеціалізовані комп'ютерні системи та робототехніка» та «Геоінформаційні системи».

Програма навчальної дисципліни складається з таких змістових модулів:

Змістовний модуль 1. Основи захисту інформації в інформаційно-комунікаційних системах.

Тема 1.1. Вступ до предмету. Основні поняття.
Тема 1.2. Базові системи захисту.
Тема 1.3. Типові вразливості систем та причини їх появи.
Тема 1.4. Шкідливе програмне забезпечення.

Змістовний модуль 2. Захист розподілених інформаційно-комунікаційних систем.

Тема 2.1. Основи безпеки інформації в комп'ютерних мережах
Тема 2.2. Засоби захисту в розподілених інформаційно-комунікаційних системах.
Тема 2.3. Безпека мережевих протоколів Internet.
Тема 2.4. Передавання інформації захищеними мережами.

1. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1.1. Метою викладання навчальної дисципліни "« Безпека інформаційно-комунікаційних систем» є розкриття сучасних концепцій, технологій та методів забезпечення безпеки інформації в інформаційно-комунікаційних системах та сформувати у курсантів та студентів знання щодо: проблем уразливості інформації в сучасних ІКС; методології захисту інформації в ІКС інформаційними технологіями захисту та захищеними технологіями оброблення; практичного використання отриманих відомостей для організації захисту інформації на об'єктах інформаційної діяльності.

1.2. Основними завданнями вивчення дисципліни «Безпека інформаційно-комунікаційних систем» є:

- засвоєння теоретичних основ процесу забезпечення безпеки інформації в інформаційно-комунікаційних системах;
- формування у студентів компетенції з використання сучасних методів та засобів захисту інформаційних ресурсів;
- отримання знань, вмінь та навичок реалізації процесів захисту розподілених інформаційно-комунікаційних системах;

1.3. У результаті вивчення дисципліни студенти повинні:

знати:

- особливості технологій побудови та функціонування між мережних екранів;
- принципи розробки політики безпеки в ІКС;
- види загроз інформації в комп'ютерних системах та мережах;
- принципи побудови та використання програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в інформаційно-комунікаційних системах;
- основні способи впровадження і супроводження системного, об'єктно-орієнтованого та прикладного програмного забезпечення інформаційно-комунікаційних систем та аналіз його ефективності;
- засоби організації розмежування доступу комп'ютерних мережах;
- механізм зараження комп'ютера adware- та spyware- програмами, комп'ютерними вірусами тощо та протидію цим процесам;
- принципи захисту локальних мереж при приєднанні до Інтернету.

вміти:

- виконати аналіз безпеки комп'ютерної системи або мережі;
- самостійно класифікувати загрози інформації та оцінювати її вразливість;
- здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- підібрати тип та структуру локальної комп'ютерної мережі;
- розробляти принципи політики безпеки в інформаційно-комунікаційних системах;
- проводити тестування основних елементів автоматизованих систем, таких .як автоматизовані робочі місця, сервери, маршрутизатори, фаєрволи та тощо;
- підібрати комплекс необхідних апаратно-програмних засобів для захисту комп'ютерної системи та мережі.

На вивчення навчальної дисципліни відводиться _90_ годин(и)/ _3,0_ кредита ECTS.

2. ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовний модуль 1. Основи захисту інформації в інформаційно-комунікаційних системах.

Тема 1.1. Вступ до предмету. Основні поняття.

Вступ. Термінологія. Завдання захисту та загрози безпеці інформації. Класифікація атак. Модель порушника.

Тема 1.2. Базові системи захисту.

Рівні інформаційно-комунікаційної системи. Функціональні сервіси безпеки та їх механізми Основні підсистеми комплексу засобів захисту.

Тема 1.3. Типові вразливості систем та причини їх появи.

Передумови виникнення вразливостей в інформаційно-комунікаційних системах. Класифікація вад безпеки. Помилки програмної реалізації систем: переповнення буфета та оброблення текстових рядків. Люки.

Тема 1.4. Шкідливе програмне забезпечення.

Класифікація шкідливого програмного забезпечення. Програмні закладки. Комп‘ютерні віруси. Мережні черв‘яки.

Змістовний модуль 2. Захист розподілених інформаційно-комунікаційних систем.

Тема 2.1. Основи безпеки інформації в комп‘ютерних мережах

Основні відомості про комп‘ютерні мережі Загрози безпеці інформації у мережах. Безпека взаємодії відкритих систем.

Тема 2.2. Засоби захисту в розподілених інформаційно-комунікаційних системах.

Архітектура захищених мереж. Міжмережні екрани. Системи виявлення атак. Системи аналізу та оцінювання вразливостей.

Тема 2.3. Безпека мережевих протоколів Internet.

Протоколи прикладного рівня. Транспортні протоколи. Протоколи IP. Протоколи керування мережею.

Тема 2.4. Передавання інформації захищеними мережами.

Захист інформації у відкритих канал зв‘язку. Віртуальні захищені мережі. Рівні реалізації віртуальних захищених мереж. Вимоги нормативної бази до реалізації віртуальних захищених мереж в Україні.

3. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. **Андрианов В.И., Бородин В.А., Соколов А.В.** "Шпионские штучки" и устройства для защиты объектов и информации: Справочное пособие. – СПб.: Лань, 1996. – 272 с.

2. **Анин Б.** Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000. — 384 с.

3. **Блам Р.** Система электронной почты на основе Linux: [пер. с англ.] – М.: Вильямс, 2001. – 456 с.

4. **Богуш В.М., Кудін А.М.** Інформаційна безпека від А до Я. - К.: МОУ, 1999. – 456 с.

5. **Гайворонський М.В., Новіков О.М.** Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с. іл.

6. **Герасименко В.А.** Защита информации в автоматизированных системах обработки данных. Т. 2. – М.: Энергоатомиздат, 1994. – 176 с.

7. **Зегжда Д.П., Ивашко А.М.** Как построить защищенную информационную систему. Том 1. - СПб: НПО «Мир и семья - 95», 1997. - 312 с.

8. **Зегжда Д.П., Ивагико А.М.** Основы безопасности информационных систем. — М.: Горячая линия — Телеком, 2000. – 452 с.

9. **Зима В., Молдовян А., Молдовян Я.** Безопасность глобальных сетевых технологий. — СПб.: БХВ-Петербург, 2001. – 320 с.

10. **Лукацкий А.** Обнаружение атак. - СПб.: БХВ-Петербург, 2001. - 624 с.

11. **Мельников В.В.** Защита информации в компьютерных системах. – М.: Финансы и статистика: Эмектроинформ, 1997. – 368 с.

12. **Олифер В.Г., Олифер Н.А.** Сетевые операционные системы – СПб.: Питер, 2001. – 672 с.

13. **Прохоров И.В., Толстой А.И.** Телекоммуникационные сети: Учебное пособие. – М.: МИФИ, 1996. – 64 с.

14. **Снейдер Йон.** Эффективное программирование TCP/IP. Библиотека программиста. – СПб.: Питер, 2001. – 320 с.

15. **Соломон Д., Руссинович М.** Внутреннее устройство Microsoft Windows 2000. — М., СПб, Харьков, Минск: Питер, Русская Редакция, 2001. – 752 с.

16. **Тимошенко А.О.** Методи аналізу та проектування систем захисту інформації: Курс лекцій. - К.: Політехніка, 2007. – 174 с.

17. **Шатт С.** Мир компьютерных сетей: [пер. с англ.] – К.: BHV, 1996. – 288 с.

18. **Eugene H. Spafford.** The Internet Worm Program: An Analysis // Purdue Technical Report CSD-TR-823 — Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-2004.

19. **Kahn D.** The Codebreakers: The Story of Secret Writing. - N.Y.: MacMillan, 1967. – 1164 p.

20. **Ken Thompson.** Reflections on Trusting Trust. // Communication of the ACM. - Vol. 27, No. 8, August 1984. - P. 761-763.

4. КРИТЕРІЇ УСПІШНОСТІ НАВЧАННЯ ТА ФОРМА ПІДСУМКОВОГО КОНТРОЛЮ

Оцінка „**відмінно”** ставиться тоді, коли курсант (студент) виявив достатньо повні знання курсу; вміє аналізувати та розробляти рішення щодо вибору та застосування засобів та методів захисту інформаційно-комунікаційних систем різних рівнів для вирішення виробничих та науково-дослідницьких завдань; матеріал обґрунтовує та викладає логічно, послідовно і переконливо.

Оцінка **„добре”** ставиться, якщо відповідь відповідає основним вимогам до оцінки „відмінно", але курсант (студент) допускає незначні неточності, які не несуть принципового характеру, не використовує чіткий план розв’язку, не застосовує знання в нестандартній ситуації, не може встановити зв'язку з раніше вивченим матеріалом .

Оцінка **„задовільно”** ставиться, якщо більша частина відповіді задовольняє вимоги до відповіді на оцінку "добре", але у відповіді виявляються значні прогалини, які не перешкоджають подальшому засвоєнню програмного матеріалу.

Оцінка **„незадовільно”** ставиться у випадку, якщо студент не оволодів основними знаннями і вміннями відповідно до вимог програми.

Форма підсумкового контролю успішності навчання

Диференційований залік.

5. ЗАСОБИ ДІАГНОСТИКИ УСПІШНОСТІ НАВЧАННЯ

Поточний контроль, який здійснюється у формі усного чи письмового опитування, виконання практичних робіт, семінари-дискусії.