МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

«**ЗАТВЕРДЖУЮ**»
Голова Вченої ради ЧДТУ
_____/ Григор О.О. /
«_____» _____ 20___ р.

ПРОГРАМА
навчальної дисципліни
«ПРОГРАМНИЙ ЗАХИСТ ІНФОРМАЦІЇ»
шифр (за ОПП) – 4.09

підготовки здобувачів освітнього ступеня «бакалавр»

Галузь знань – 1701 «Інформаційна безпека»

Напрям – 6.170103 «Управління інформаційною безпекою»

2016 рік

РОЗРОБЛЕНО ТА ВНЕСЕНО КАФЕДРОЮ:
Інформаційної безпеки та комп’ютерної інженерії

Протокол засідання кафедри № __ від _____ 20 __ р.

РОЗРОБНИКИ ПРОГРАМИ:

асистент Лавданський А.О.

асистент Бреус Р.В.

Обговорено та рекомендовано до затвердження методичною комісією факультету інформаційних технологій і систем

«____» _____ 20___ р., протокол №__

ПОГОДЖЕНО

Навчально-методичний відділ _____ /_____/
підпис *ПІБ*

«____» _____20___ р.

ВСТУП

Програма навчальної дисципліни «Програмний захист інформації» складена відповідно до освітньо-професійної програми підготовки здобувачів освітнього ступеня «бакалавр»
з галузі знань – 1701 «Інформаційна безпека»,
за напрямом підготовки – 6.170103 «Управління інформаційною безпекою».

Предметом вивчення навчальної дисципліни «Програмний захист інформації» є забезпечення є формування знань та вмінь визначених освітньо-кваліфікаційною характеристикою, за сукупністю й рівнями їхньої сформованості, необхідними для вирішення професійних завдань.

Міждисциплінарні зв'язки:

Вивчення курсу базується на знаннях, які студенти отримали у процесі вивчення таких дисциплін, як інформатика, програмування, інформаційна безпека держави, основи національної безпеки.

Мета та завдання навчальної дисципліни:

1. Навчальна дисципліна має за мету вивчення студентами основ забезпечення програмного захисту інформації. Наукову основу дисципліни складають загальні принципи навчання в вищому навчальному закладі, які визначають знання, уміння та навички студентів, останні досягнення у галузі вищої освіти та практика управління в системах спеціального призначення.

2. Основні завдання навчальної дисципліни .

Згідно з вимогами освітньо-професійної програми студентів після засвоєння навчальної дисципліни мають продемонструвати такі результати навчання:

Знання:

- Політика безпеки.
- Механізми та служби захисту.
- Особливості комп'ютерних вірусів.
- Особливості та призначення руткітів.
- Особливості віддалених мережевих атак.
- Розвиток технологій міжмережевих екранів
- Моделі систем виявлення атак і вторгнень.
- Віртуальні приватні мережі.
- Аналіз програмних реалізацій.
- Захист програм від аналізу.
- Програмні закладки, шляхи їх впровадження.
- Передумови для впровадження програмних закладок.

- Комп’ютерні віруси.
- Організаційні та адміністративні міри антивірусного захисту.

Уміння:

- Виявлення існуючих та потенційних загроз у сфері програмного захисту інформації.
- Виявляти та усувати шкідливі програми.
- Використовувати світовий досвід щодо програмного захисту інформації для його впровадження в Україні.
- Встановлення антивірусних програм.
- Експертиза якості реалізації програмних засобів забезпечення інформаційної безпеки .
- Виявлення уразливостей програмного забезпечення.
- Виявлення шкідливого програмного забезпечення.
- Оцінка небезпеки шкідливого програмного забезпечення.

Досвід:

- Проводити дослідження у сфері забезпечення програмного захисту інформації.
- Використовувати новітні антивірусні програми для захисту інформації.
- Знаходити шляхи протидії програмним закладкам.
- Планування роботи по локалізації наслідків та припинення виявленої атаки.

На вивчення навчальної дисципліни відводиться 252 години 7 кредитів ЄКТС.

1. Інформаційний обсяг навчальної дисципліни

Змістовий модуль №1 Забезпечення безпеки міжмережевої взаємодії.

Тема 1. Лекція №1 Вступ до дисципліни «Програмний захист інформації».

Тема 1.1 Лабораторна робота №1 Робота з сучасними архіваторами. Застосування антивірусних програм для захисту комп’ютерів від вірусів

Тема 2. Лекція №2 Мережева та міжмережева взаємодія. Політика безпеки.

Тема 2.1. Лабораторна робота № 2 Реалізація дискреційної моделі політики безпеки.

Тема 3. Лекція №3 Основи управління ризиками. Поняття аудиту інформаційної безпеки.

Змістовий модуль №2 Основи захисту від несанкціонованого доступу.

Тема 1. Лекція №4 Основи захисту комп'ютера від несанкціонованого доступу. Комп'ютерні віруси.

Тема 1.2. Лабораторна робота № 3 Кількісна оцінка стійкості парольного захисту.

Тема 2. Лекція №5-6 Хакерські новітні технології. Руткіти.

Змістовний модуль № 3 Боротьба з небезпечним програмним забезпеченням.

Тема 1. Лекція 7-9 Потенційно небезпечне програмне забезпечення.

Тема 1.1. Лабораторна робота № 4 Захист баз даних на прикладі MS Access.

Тема 2 Лекція № 10 Елементи захисту від шкідливого програмного забезпечення. Новітні технології боротьби з шкідливим програмним забезпеченням.

Змістовний модуль № 4 Технології міжмережевого екранування.

Тема 1 Лекція № 11-12 Розвиток технологій міжмережевих екранів.

Тема 2 Лекція №13 Нові покоління міжмережевих екранів.

Тема 3 Лекція №14 Обхід міжмережевих екранів. Вимоги та показники захищеності міжмережевих екранів.

Тема 3.1. Лабораторна робота №5 Застосування антивірусного безкоштовного сертифікованого програмного забезпечення Avast.

Змістовний модуль № 5 Аналіз програмних реалізацій.

Тема 1. Лекція №15 Основі методи аналізу програмного забезпечення.

Тема1.1. Лабораторна робота № 1 Порівняльний аналіз антивірусного програмного забезпечення.

Тема 2. Лекція №16-17 Особливості аналізу деяких видів програм.

Тема 2.1. Лабораторна робота № 2 Особливості боротьби з потенційно небезпечними програмами на основі Spyware.

Тема 3. Лекція №18-19 Захист програм. Методи ускладнення структури програм.

Тема 3.1. Лабораторна робота № 3 Програмні закладки. Клавіатурний шпигун.

Змістовий модуль №6 Програмні закладки. Шляхи їх застосування. Засоби та методи протидії програмним закладкам.

Тема 1. Лекція №20 Особливості програмних закладок. Основні моделі взаємодії програмних закладок.

Тема 1.1. Лабораторна робота № 4 Інвентаризація ресурсів комп'ютерних систем.

Тема 2. Лекція №21 Методи застосування програмних закладок.

Тема 2.1. Лабораторна робота № 5 Використання засобів захисту текстових документів.

Тема 3. Лекція №22 Комп'ютерні віруси як особливий клас програмних закладок.

Тема 3.1. Лабораторна робота №6 Тестування та верифікація програм. Тестування «чорного ящика».

2. Рекомендована література

1. Проскурін В. Г. П824 Захист програм і даних: навч, посібник

для студ. закладів вищ. проф. освіти / В. Г. Проскурін. 2-е вид., стер. — М. : Издательский центр «Академия», 2012. 208 с.

2. Шрайбер С. Недокументированные возможности Windows 2000 / С. Шрайбер. - СПб. : Питер, 2002.

3. Проскурин В. Г. Защита в операционных системах / *В. Г.* Проскурин, С. В. Крутов, И. В. Мацкевич. — М. : Радио и связь, 2000.

4. Девянин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин — М. : Радио и связь, 2006.

Додаткова:

1. Проскурин В. Г. Защита в операционных системах / В. Г. Проскурин, С. В. Крутов, И.В.Мацкевич. — М. : Радио и связь, 2000.

2. Белов Е.Б. Основы информационной безопасности / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — М.: Горячая линия — Телеком, 2006.

3. Лукацкий А. В. Обнаружение атак / А. В.Лукацкий. — СПб. : БХВ-Петербург, 2001.

4. Форд Д. Л. Персональная заищита от хакеров. Руководство для начинаюших: пер. с англ. / Д.1Л.Форд. — Р. м.: КУДИЦ-ОБРАЗ, 2002.

Інтернет ресурси:

5. Віруси та антивіруси, http://83.102.140.71/bezopasnost/virusy_i_ antivirusy.
6. Поздеев В. Вредоносные программы и вирусы/В. Поздеев http://www. whatis. ru/razn/razn20. shtml.
7. Проскурін В. Г. Проблеми захисту мережевих з'єднань в Windows NT/В. Г. Проскурін. http://bugtraq. ru/library/intemals/admintrap. html.

3. Інформаційні ресурси (за необхідністю)

4. Форма підсумкового контролю успішності навчання

Денна форма навчання – підсумковий модульний контроль, іспит в кінці 6 семестру та залік в кінці 7 семестру.

1. **Засоби діагностики успішності навчання**

Оцінювання студентів проводяться згідно тематики вивчення дисципліни. Ці заходи мають на меті поглибити та закріпити знання, отримані студентами на лекціях, лабораторних роботах та в процесі самостійної

роботи над навчальною та науковою літературою, рекомендованою викладачем, а також виробити у тих, хто навчається, уміння пошуку, узагальнення та викладання навчального матеріалу.

Підсумкові бали (оцінки) за кожне заняття вносяться викладачем до журналу занять навчальної групи. Одержані ними оцінки за окремі заняття враховуються при визначенні підсумкової оцінки (рейтингу) з даної навчальної дисципліни. Проводиться поточний контроль (усне та письмове опитування), виконання лабораторного завдання, підсумковий письмовий тест, екзамен в кінці 6-го семестру, залік в кінці 7-го семестру.

6. Методичні рекомендації

Реалізація цільової настанови дисципліни здійснюється чіткою, взаємопов'язаною системою лекційних та практичних занять, проведенням індивідуальних та групових консультацій, а також самостійною роботою над вивченням навчального матеріалу.

На лекціях розглядаються найбільш складні теоретичні питання, які носять проблематичний характер і відображають актуальні питання щодо забезпечення програмного захисту інформації.

На лабораторних заняттях студенти отримають навички в рішенні необхідних завдань програмного захисту інформації.

На самостійних заняттях під керівництвом викладача студентами виконуються завдання з метою поглиблення та закріплення вивченого матеріалу.

Знання навчального матеріалу дисципліни та практичні навички, здобуті студентами при вивченні шести змістовних модулів, оцінюються на всіх видах занять шляхом проведення поточного опитування за бальними критеріями, а також проведенням семестрового іспиту згідно «Положення про РСО» в кінці 6-го семестру та заліку в кінці 7-го семестру.

Навчально-матеріальне забезпечення.

1. Основна та допоміжна література.