МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

«**ЗАТВЕРДЖУЮ**»
Голова Вченої ради ЧДТУ
_____/ Григор О.О. /
«_____» _____ 2017 р.

ПРОГРАМА

навчальної дисципліни

«Основи технічного захисту інформації»

шифр (за ОПП) - 4.02

підготовки здобувачів освітнього ступеня «бакалавра»

напряму підготовки 6.170103 «Управління інформаційною безпекою»

2017 рік

РОЗРОБЛЕНО ТА ВНЕСЕНО КАФЕДРОЮ
____інформаційної безпеки та комп'ютерної інженерії

Протокол засідання кафедри № 1 від 28. 09. 2017 р.

РОЗРОБНИКИ ПРОГРАМИ:

к.т.н., доцент **Швидкий Валерій Васильович**
асистент **Лавданський Артем Олександрович**

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

Протокол № 2 від 15. 09. 2017 р.

ПОГОДЖЕНО
Навчально-методичний відділ _____/ _____ /
«____»_____ 2017 р.

ВСТУП

Програма навчальної дисципліни «**Основи технічного захисту інформації**» складена відповідно до освітньо-професійної підготовки здобувачів освітнього ступеня «бакалавр» напряму підготовки 6.170103 «Управління інформаційною безпекою»

Предметом вивчення навчальної дисципліни є принципи побудови технічних засобів захисту інформації, забезпечення захисту об'єктів, споруд, приміщень в яких здійснюється обробка, збереження чи транспортування інформації з обмеженим доступом. **Міждисциплінарні зв'язки**. Вивчення курсу базується на знаннях, що отримані студентами у процесі вивчення дисциплін: "Математика", "Інформатика", "Захист інформації в комп'ютерних системах".

Основи технічного захисту інформації як навчальна дисципліна закладає основи вивчення дисципліни "Комп'ютерні системи" в частині забезпечення їх безпеки.

Зв'язок з названими дисциплінами полягає в тому, що забезпечується формування у студентів навичок проектування та розробки систем захисту автоматизованої комп'ютерної системи та інформації в ній від несанкціонованого доступу, а також вмінь застосовувати технічні засоби забезпечення безпеки системи, об'єктів і інформації в ній.

Мета та завдання навчальної дисципліни. Метою викладання навчальної дисципліни Основи технічного захисту інформації є вивчення теоретичних основ, практичних методів забезпечення безпеки зберігання, обробки і транспортування інформації з обмеженим доступом, а також питань пов'язаних з життєвим циклом, підтримкою і супроводом таких систем.

Основними ***завданнями*** вивчення дисципліни Основи технічного захисту інформації є підвищення рівня знань студентів при розробці інформаційних систем забезпечення безпеки, що полягає в наступному:

1) Дати студентам такі базові знання з теорії систем захисту інформації:

- основні поняття про канали витоку інформації і принципи побудови засобів блокування каналів витоку;
- основні поняття про закладні пристрої, що забезпечують доступ до інформації, що циркулює в автоматизованій комп'ютерній системі;
- принципи побудови технічних засобів, що забезпечують виявлення закладних пристроїв;
- фізична природа утворення каналу витоку у відведенні ланцюги і відкритий радіо простір (ВРП);
- методи придушення паразитичного електромагнітного випромінювання та наводок, розв'язка ланцюгів відкритої і закритої інформації, екранування пристроїв, блоків, приміщень;
- витік закритої інформації у відкриті мережі, засоби блокування каналу витоку;
- радіо портрет об'єкту, ідентифікація об'єкту за портретом, демаскування об'єкту, протидія демаскуванню;
- теоретичні основи проектування систем захисту інформації.

2) Прищепити і відпрацювати у студентів вміння і навички створення систем захисту об'єктів, будівель та приміщень, обладнаних технічними засобами збереження, обробки і транспортування інформації з обмеженим доступом.

В результаті вивчення курсу студент повинен *знати*:

- канали витоку інформації з обмеженим доступом;
- фізичні процеси в каналах витоку, що забезпечують винесення відкритих даних у відкритий радіо простір, ланцюги електроживлення, контури заземлення і в канал зв'язку;
- принципи побудови закладних пристроїв («жучків»), що забезпечують реєстрацію, зберігання та передачу порушнику інформації з охоронної зони;

- принципи і засоби виявлення закладних пристроїв;
- принципи і засоби, що забезпечують несанкціоноване дистанційне зчитування аудіо і відео сигналів, що циркулюють в охоронній зоні;
- принципи і засоби, що забезпечують придушення дистанційно зчитувальних аудіо і відео небезпечних сигналів, що циркулюють в охоронній зоні;
- принципи побудови технічних засобів виявлення каналів витоку інформації на кордоні охоронної зони;
- принципи і засоби контролю радіо простору по радіо портрету об'єкта;
- принципи і засоби маскування залишків небезпечного сигналу;
- оцінка небезпечного впливу на організм люди систем просторового зашумлення, визначення допустимого рівня шуму маскування;
- оцінка впливу на організм люди систем екранування приміщень, оснащених засобами зберігання, обробки і транспортування інформації з обмеженим доступом..

В результаті вивчення курсу студент повинен ***вміти***:

- природа утворення каналу витоку інформації в: відкритий радіо простір, мережу електроживлення, в ланцюги заземлення і в канал зв'язку;
- професійно використовувати отримані знання при спостереженні за каналами витоку з охоронної зони, забезпечувати підтримку допустимого рівня небезпечного сигналу на кордоні охоронної зони;
- володіти методикою пошуку «жучків» в межах охоронної зони;
- володіти методиками захисту від прослуховування приміщень в середині охоронної зони, засобами технічної розвідки, розміщеними поза охоронною зоною;
- володіти методами протидії дистанційному зчитуванню аудіо і відео сигналів, що циркулюють в охоронній зоні;
- вміти виконувати розрахунки по визначенню: зони радіовидимості джерела небезпечного сигналу, рівня небезпечного сигналу на кордонах охоронної зони, рівня шуму, що маскує залишки небезпечного сигналу;
- володіти методами контролю радіо портрета об'єкту, що охороняється і заходів підтримки його статистичної стійкості. Правові аспекти системи захисту інформації

На вивчення навчальної дисципліни відводиться 120 годин 4 кредитів ЄКТС.

1. Інформаційний обсяг навчальної дисципліни

Змістовний модуль №1. Основний зміст дисципліни і його правові основи

Тема 1. Вступ

Основні Поняття. Інформація без обмеження доступу і інформація з обмеженим доступом. Конфіденційна і секретна інформація, Поняття конфіденційної інформації як об’єкту охорони особистої, лікарської, комерційної, виробничої і тому подібних видів таємниць- об'єктів захисту в рамках даного курсу.

Тема 2. Правова база систем захисту комп'ютерних систем

Правова база: закон про інформацію, закон про захист автоматизованої системи та інформації в ній. Основні поняття і визначення: об'єкт охорони, охоронна зона, периметр охоронної зони, розмежування доступу, порушник (режиму розмежування доступу), втрата інформації, витік інформації, блокування інформації, підробка інформації та даних.

Тема 3. Закладні пристрої («жучки») для несанкціонованого доступу до інформації

Принцип побудови закладних пристроїв (закладок) для читання охоронюваних даних телекомунікаційних систем, аудіо і відео інформації, породжених в охоронній зоні. Канали виносу інформації закладками: радіо канал, мережа електроживлення. Радіо портрет об'єкта, (з закладками і без закладок), контроль сигналів в відведених ланцюгах: заземлення, електроживлення, лінія зв'язку (в абонентських і з'єднувальних лініях). Придушення сигналів, що генеруються закладками.

Тема 4. Технічні засоби виявлення закладок

Контроль радіо портрету об'єкта: організація системи контролю, технічні засоби контролю. Панорамні радіоприймачі і їх місце в моніторингу радіо простору. Контроль сигналу у відведених ланцюгах. Придушення сигналів, що генеруються закладками. Маскування (зашумлення) сигналів, що генеруються закладками. Технічні засоби виявлення сигналів, що породжуються закладками в радіо просторі, технічні засоби виявлення сигналів, що породжуються закладками в мережах електроживлення.

Змістовний модуль №2 Витік небезпечного сигналу в навколишній радіо простір

Тема 1. Фізична природа утворення каналу витоку в радіо простір

Двоїстість функцій перемикачів схем: загальновідоме функціональне призначення (схеми І, АБО, НЕ, тригери і т.п.) і приховане (генератори високочастотних паразитичних сигналів, модулятори паразитичного сигналу сигналом конфіденційних даних). Двоїстість функцій друкованих провідників друкованих плат: загальновідоме функціональне призначення (з'єднання між собою виходів електронних компонент вузлів і блоків) і приховане (перетворювачі акустичних коливань в електричний сигнал, антени, що забезпечують винесення модульованих сигналів в радіо простір). Фізична природа виникнення витоку інформації в мережу електроживлення, в контур заземлення та лінії зв'язку. Рівні сигналів в каналах витоку, спектр сигналу в каналі витоку. Радіо портрет охоронного об'єкту, оцінка об'єкта по портрету, боротьба з демаскуванням об`єкту за основними параметрами об'єкту.

Тема 2. Методи придушення небезпечних сигналів в каналі витоку

Екранування ланцюгів, блоків, пристроїв, приміщень. Паразитна генерація в перемикальних схемах. Методи зриву паразитної генерації. Поширення паразитних сигналів по ланцюгах електроживлення і шинам заземлення в вузлах і блоках. Придушення паразитних сигналів в ланцюгах живлення і заземлення. Зашумлення ланцюгів з паразитними сигналами. Винесення паразитних сигналів в навколишній радіо простір друкованими провідниками друкованих плат. Зашумлення паразитних сигналів у вузлах і блоках комп'ютерних систем. Придушення небезпечного сигналу до допустимого рівня на кордоні охоронної зони (до рівня шуму в каналі витоку на кордоні охоронної зони). Маскування шумом не придушених залишків небезпечного сигналу.

Тема 3. Методи зменшення рівня небезпечних сигналів

Види екранів, оцінка ступеня придушення небезпечного сигналу. Екранування приміщення, пристроїв, блоків комп'ютерних систем. Забезпечення електрогерметичності екранованих вузлів, блоків, приладів. Порушення електрогерметичності за рахунок: вентиляційних отворів, органів управління і сигналізації, роз'ємів. Оптична розв'язка вузлів, блоків і приладів. Генератори зашумлення, принципи побудови. Панорамні радіоприймачі. Розвідувальні антени. Екрановані приміщення для оцінки рівня і спектра паразитного випромінювання компонентами комп'ютерних систем.

Тема 4. Забезпечення безпеки функціонування об'єкта, будівлі, приміщення

Охорона периметра об'єкта: засобами служби охорони (паркани, контрольно слідова смуга) і технічними засобами спостереження (відеокамери, датчики руху). Охорона

будівель (вікон, дверей). Засоби розвідки: засоби оптичної розвідки, віддалене зчитування мовних сигналів, засоби контролю радіо портрета. Блокування засобів розвідки.

Змістовний модуль №3 Фізична природа утворення каналу витоку в мережу електроживлення і в ланцюги заземлення

Тема 1. Захисне та сигнальне заземлення

Об'єднання і поділ цих ланцюгів. Умови, що визначають необхідність об'єднання / роз'єднання ланцюгів.

Виконання контуру заземлення: в межах охоронної зони і поза охоронної зони. Фактори що впливають на вибір місця розташування - радіус охоронної зони. Особливості організації контуру заземлення для мобільних комп'ютерних систем обробки інформації з обмеженим доступом. Норми на перехідний опір ланцюга заземлення, забезпечення і контроль цих норм. Оцінка рівня небезпечного сигналу в ланцюзі заземлення при використанні контуру заземлення розташованого поза охоронної зони. Маскування (зашумлення) небезпечного сигналу в ланцюзі заземлення. Генератори струму зашумлення, принцип побудови, основні технічні характеристики.

Тема 2. Утворення каналу витоку в мережі електроживлення

Організація системи електроживлення великих систем і об'єктів. Організація системи електроживлення великих вузлів комп'ютерних систем, що обробляють інформацію з обмеженим доступом. Організація системи електроживлення невеликих комп’ютерних об'єктів (типу абонентський термінал, мобільних об'єктів). Резервування системи електроживлення. Фізичні процеси в комп'ютерному обладнанні, що призводять до утворення каналу витоку. Блокування каналу витоку шляхом переходу на електроживлення постійним струмом. Електромашинні генератора, їх властивості і область застосування. Системи безперебійного живлення, принцип побудови, область застосування. Маскування (зашумлення) небезпечного сигналу в ланцюзі електроживлення, розміщення трансформаторної підстанції в охоронній зоні. Генератори шуму для зашумлення ланцюгів електроживлення.

Змістовний модуль №4 Утворення каналу витоку в лінії зв'язку

Тема 1. Природа фізичних процесів, що призводять до витоку інформації в лінії зв'язку

Фізичні процеси, в комп'ютерній системі, що призводять до просочування небезпечного сигналу в лінії зв’язку від всіх вузлів і блоків, що входять в систему. Оцінка ефективності блокування кожного вузла і блоку або сумарного наведеного сигналу.

Композиції різних представлень небезпечного сигналу. Перехресна і взаємна модуляція небезпечних сигналів породжених різними пристроями, блоками і приладами комп'ютерної системи. Комбінаційні продукти і їх спектр. Концентрація небезпечних сигналів на кордоні охоронної зони (з внутрішньої сторони зони).

Тема 2. Блокування витоку в лінії зв'язку

Поділ об'єкта на зону небезпечного сигналу, зону відкритого сигналу і зону обслуговування. Основні ознаки зон: зона небезпечного сигналу - безлюдна зона з доступом тільки при припиненні обробки інформації з обмеженим доступом, зона відкритого сигналу - безлюдна зона, але з дозволеним доступом персоналу за вказівкою адміністратора системи. Зона обслуговування - зона розміщення обслуговуючого персоналу і адміністратора системи. Технічні засоби поділу зон: оптоелектронні розв'язки, фільтри придушення позасмугової компоненти небезпечного сигналу на кордоні охоронної зони. Генератори маскування (зашумлення) смугової складової небезпечного сигналу. Рівень маскуючого шуму і його вплив на достовірність передачі даних.

2. Рекомендована література

Основна

1.Вартанесян В.А. Радиоэлектронная разведка.М, Воениздат 1991– 440 с.
2. Волин М.Л. Пакразитные связи и наводки. М.Сов.Радио 1965-340стр
3. Киселев А.Е. Коммерческая безопасность М.ИнфоАрт, 1993-370стр.
4. Технические средства разведки. Под редакциейВ.И.Мухина. М.РВСН,1992 - 352 с.
5. Ярочкин В.И.Технические каналы утечки.М.ИПКИР,1994 - 240 с.

Додаткова

1. В..А. Герасименко Защита информации в автоматизированных системах обработки данных. - М.: Энергоиздат, 1994.
2. В. Жельников "Криптография от папируса до компьютера". - М.:ABF, 1996.
3. Д.П. Зегжда, А.М.Ивашко "Как построить защищенную информационную систему". - СП.: "Мир и семья-95", 1997.
4. В.Д. Медведовский, П.В. Семьянов, В.В. Платонов "Атака через INTERNET". - СП.: "Мир и семья-95", 1997.
5. Мельников В.В. "Защита информации в компьютерных системах". - М.: "Финансы и статистика", 1997.
6. Н.Т.Березюк, А.Г.Андрущенко и др. "Кодирование информации" Харьков, "Вища школа", 1978.
7. В.В. Домарев "Защита информации и безопасность компьютерных систем" - К.: Издательство "Диасофт", 1999. - 480с.
8. Эд Таили "Безопасность персонального компьютера" - Мн.: ООО "Попурри", 1997.-480 с.:ил.
9. Котов П.А. "Повышение достоверности передачи цифровой информации"-М.: "Связь", 1966, 184с.

3. Форма підсумкового контролю успішності навчання

Залік у 5 семестрі 3-го курсу навчання.

4. Засоби діагностики успішності навчання.

Поточний контроль здійснюється шляхом проведення поточних усних опитувань і виконання лабораторних робіт.

Модульний контроль здійснюється шляхом проведення підсумкових модульних робіт. В процесі модульного контролю оцінюються знання студентів за кожний змістовний модуль.

Підсумковий контроль здійснюється шляхом проведення *заліку.*