МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

"**ЗАТВЕРДЖУЮ**"
Завідувач кафедри
інформаційної безпеки та
комп'ютерної інженерії

_____/Федотова-Півень І.М./
"_____"_____2017 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Основи технічного захисту інформації»

підготовки здобувачів освітнього ступеня «бакалавр»

напряму підготовки 6.170103 «Управління інформаційною безпекою»

2017

Робоча програма навчальної дисципліни «Основи технічного захисту інформації» підготовки здобувачів освітнього ступеня «бакалавр» за напрямом підготовки 6.170103 «Управління інформаційною безпекою» - 11 стор.

Робоча програма складена на основі програми навчальної дисципліни «Основи технічного захисту інформації», шифр (за ОПП) – 4.02

Розробники програми:

к.т.н., доцент, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Швидкий Валерій Васильович;

асистент кафедри інформаційної безпеки та комп'ютерної інженерії Лавданський Артем Олександрович.

Робоча програма затверджена на засіданні кафедри *інформаційної безпеки та комп'ютерної інженерії*

Протокол від " ____ " _____2017 року № _____ .

ЗМІСТ

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, спеціалізація, 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>Кількість кредитів – 4</td><td>Галузь знань
1701 «Інформаційна безпека»</td><td colspan="2">Вибіркова</td></tr>
<tr><td rowspan="4">Загальна кількість годин - 34</td><td rowspan="4">Напрям підготовки
6.170103 - «Управління інформаційною безпекою»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>2017</td><td>-</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>5</td><td>-</td></tr>
<tr><td rowspan="11">Змістових модулів – 4</td><td rowspan="11">Рівень вищої освіти
перший (бакалаврський)</td><td colspan="2">Лекції</td></tr>
<tr><td>16 год.</td><td>-</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 год.</td><td>-</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>88 год.</td><td>-</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td>залік</td><td>-</td></tr>
</table>

Примітка:

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить 36% для денної форми навчання.

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою викладання навчальної дисципліни «Основи технічного захисту інформації» є вивчення теоретичних основ, практичних методів і засобів побудови систем захисту інформації с обмеженим доступом від навмисних або ненавмисних дій фізичних чи юридичних осіб, спрямованих на отримання доступу до інформації, до якої ці особи недопущені, а також питань пов'язаних з життєвим циклом, підтримкою і супроводом таких системи захисту.

Основними завданнями вивчення дисципліни "Основи технічного захисту інформації" є підвищення рівня знань студентів в області захисту

інформації при розробці інформаційних систем збереження, обробки і транспортування даних з обмеженим доступом, що полягає в наступному:

1) дати студентам такі базові знання з теорії систем збереження, обробки і транспортування даних з обмеженим доступом:

– принципи побудови інформаційних систем, збереження, обробки і транспортування даних з обмеженим доступом;
– забезпечення заданого рівня небезпечного сигналу на кордоні охоронної зони;
– відомості по принципам побудови закладних пристроїв і методів їх пошуку;
– технології радіоелектронної розвідки;
– теоретичні основи виносу небезпечного сигналу за рахунок паразитних електромагнітних випромінювань і наводок;
– принципи побудови технічних засобів блокування каналів витоку.

2) Прищепити і відпрацювати у студентів вміння і навички створення систем збереження, обробки і транспортування даних з обмеженим доступом та методів протидії всім видам технічної розвідки.

3. КОМПЕТЕНЦІЇ, ЩО ФОРМУЮТЬСЯ ПІСЛЯ ОПАНУВАННЯ ДИСЦИПЛІНИ

Загальні компетенції (ЗК6, ЗК14):

- Здатність використовувати сучасні інформаційно-комунікаційні технології (збір і аналіз інформації в комп'ютерних мережах, застосування інтернет-ресурсів та програмних засобів) для побудови систем і технічних засобів захисту інформації з обмеженим доступом;
- Здатність до постійного саморозвитку, підвищення своєї кваліфікації і професійної майстерності.

Професійні компетентності ($ПК_8$, $ПК_9$, $ПК_{19}$):

- Розробляти заходи та технічні засоби захисту комп'ютерних систем і інформації в них від несанкціонованого доступу до інформаційних ресурсів та баз даних обмеженого доступу, а також модулі або компоненти засобів захисту інформації з обмеженими доступом;
- Розробляти модулі або компоненти засобів захисту інформації з обмеженим доступом від несанкціонованого доступу та вміти використовувати спеціалізовані захищені бази даних для накопичення та обробки інформації з обмеженим доступом.
- Здатність використовувати знання, уміння й навички в галузі інформаційної безпеки для теоретичного засвоєння загально-професійних дисциплін і вирішення практичних завдань.

4. ТЕМАТИЧНИЙ ПЛАН 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»)

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 них), 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.

.

5. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви тем	Кількість годин									
	денна форма					заочна форма				
	Усього	у тому числі				Усього	у тому числі			
		Лекції	Прак. роботи	Лаб. роботи	Сам. робота		Лекції	Прак. роботи	Лаб. роботи	Сам. робота
Змістовий модуль №1										
Тема 1. Вступ		1								
Тема 2. Закладні пристрої («жучки»)		1		2	5					
Тема 3. Засоби виявлення закладок		2		2	5					
Разом за модулем	**18**	**4**	**-**	**4**	**10**	**-**	**-**	**-**	**-**	**-**
Змістовий модуль №2										
Тема 1. Канал витоку в радіо простір		1			2					
Тема 2.Придушення небезпечних сигналів		1		2	10					
Тема 3. Зменшення рівня небезпечних сигналів		1			10					
Тема 4. Безпека функціонування об'єкта		1		2	10					
Разом за модулем	**38**	**4**	**-**	**4**	**30**	**-**	**-**	**-**	**-**	**-**
Змістовий модуль №3										
Тема 1. Заземлення		2		**2**	**10**					
Тема 2.Канал витоку в мережі електроживлення		2		**2**	**10**					
Разом за модулем	**28**	**4**	**-**	**4**	**20**	**-**	**-**	**-**	**-**	**-**
Змістовий модуль №4										
Тема 1. Виток інформації в лінії зв'язку		2		2	14					
Тема 2 Блокування витоку в лінії зв'язку		2		2	14					
Разом за модулем	**36**	**4**	**-**	**4**	**28**	**-**	**-**	**-**	**-**	**-**
Усього годин	***120***	***16***	**-**	***16***	***88***					

6. ТЕМИ ЛАБОРАТОРНИХ РОБІТ

№ з/п	Назва теми	Кількість годин
1.	Розробка моделей охоронного об'єкту, визначення комплексу вимог з безпеки	2
2.	Оцінка рівня небезпечного сигналу в ОРП, розробка заходів по його блокування	2
3.	Оцінка рівня небезпечного сигналу в ланцюзі заземлення, розробка заходів по його блокуванню	2
4.	Оцінка рівня небезпечного сигналу в мережі електроживлення, розробка заходів по його блокуванню	2
5.	Оцінка рівня небезпечного сигналу в лінії зв'язку, розробка заходів по його блокуванню	2
6.	Розробка заходів забезпечення захисту приміщення від несанкціонованого доступу до інформації по каналах витоку	2
7.	Розробка заходів, що забезпечують поділ зон (небезпечного і безпечного сигналів)	2
8.	Розробка генератора просторового зашумлення	2
	Разом:	**16**

7. ТЕМИ ДЛЯ САМОСТІЙНОЇ РОБОТИ

№ з/п	Назва теми	Кількість годин
1	Логарифмічна міра вимірювання параметрів сигналу	8
2	Спектри і властивості перетворення Фур'є	8
3	Прийом слабких сигналів (когерентний, некогерентний, оптимальний, неоптимальний)	10
4	Розвідувальні антени, розвідувальні приймачі	8
5	Принципи побудови закладних пристроїв, виявлення закладних пристроїв	10
6	Фактори, що демаскують закладні пристрої	8
7	Виявлення закладок по портрету об'єкта	8
8	Виявлення небезпечного сигналу по портрету об'єкта	10
9	Виявлення небезпечного сигналу в відведених ланцюгах	10
10	Підготовка до захисту лабораторних робіт	8
	Разом:	**88**

8. ПЕРЕЛІК ІНДИВІДУАЛЬНИХ НАВЧАЛЬНО-ДОСЛІДНИХ ЗАВДАНЬ

Не передбачено навчальною програмою дисципліни.

9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Лысов А.В.,Остапенко А.Н. Промышленный шпионаж в России, методы и средства. Выпуск 3. Санкт Петербург,1994г. – 104 с.
2. Ярочкин В.И.Технические каналы утечки информации. М., Изд-во: НИКИР,1994г. – 280 с.
3. Ярочкин В.И. Служба безопасности коммерческого предприятия. М., Изд-во: «Ось-89»,1995г. – 230 с.
4. Атакующая спецтехника Украинской фирмы «Вече», М.,сб. Защита информации№2,1994г. 90 с.
5. Атраджев М.И. и др. Борьба с радиоэлектронными средствами.М.,Воениздат, 1992г.-350с.
6. Вакин С.А.,Шустов Л,И., Основы радиопротиводействия радиотехнической разведке.М., Сов. Радио,1998г.
7. Кащеев В.И. Мониторинг телефонных сетей.М.,Системы безопасности,1995г.№1-180с.
8. http://trident-ua.info/novyny/vijna-na-shodi средства радиоэлектронной борьбы Украинской армии
9. Хорев, А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации — М.: Гостехкомиссия РФ, 1998
10. Н.И. Юсупова «Защита информации в вычислительных системах» Уфа 2000

Додаткова

1. Демин, В. П. и др. Радиоэлектронная разведка и радиомаскировка М.: Изд-во МАИ, 1997
2. Кулаков, В. Г., Гаранин М. В., Заряев А. В. и др. Информационная безопасность телекоммуникационных систем (технические аспекты). Учебное пособие для вузов — М.: Радио и связь, 2004
3. Куприянов, А. И. Радиоэлектронные системы в информационном конфликте — М.: Вузовская кн., 2003
4. Лагутин, В. С., Петраков А. В. Утечка и защита информации в телефонных каналах — М.: Энергоатомиздат, 1996
5. Мельников, Ю. П. Воздушная радиотехническая разведка — М: Радиотехника, 2005
6. Меньшаков, Ю. К. Защита объектов и информации от технических средств разведки — М.: РГГУ, 2002 ISBN 5-7281-0487-8
7. Радзиевский А. Г., Сирота А. А. Теоретические основы радиоэлектронной разведки. — М: Радиотехника 2004
8. В.С.Барсуков «Безопасность: технологии, средства, услуги» М. Кудиц - образ 2001

9. М. Бэнкс «Психи и маньяки в Интернете: Руководство по выживанию в кибернетическом пространстве» СПБ «Символ» 1998
10. С.Н. Гриняев «Интеллектуальное противодействие информационному оружию» М «Синтег» 1999
11. М.Б. Зуев «INTERNET: Советы бывалого чайника» М. ООО «Лаборатория Базовых Знаний» 1998

10. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

1. Програма навчальної дисципліни "Основи технічного захисту інформації" Швидкий В.В.. – ЧДТУ, 2017р.
2. Робоча програма "Основи технічного захисту інформації" / Швидкий В.В.– ЧДТУ, 2017р.
3. Тематичний план з дисципліни "Основи технічного захисту інформації".
4. Тестові завдання з дисципліни "Основи технічного захисту інформації".
5. Перелік питань для підсумкового контролю.
6. Методичні вказівки до виконання лабораторних робіт з дисципліни "Основи технічного захисту інформації" (електронний ресурс).

11. ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ

Microsoft Office Access, SQL (Structured query language), Visual Prolog

12. КРИТЕРІЇ ОЦІНЮВАННЯ НАВЧАЛЬНИХ ДОСЯГНЕНЬ СТУДЕНТІВ

Для студентів денної форми навчання	
Вид навчальної роботи	Кількість балів *максимум*
Постійна частина	
ЗМІСТОВИЙ МОДУЛЬ №1 Основний зміст дисципліни і його правові основи - 18 годин	
Виконання лабораторної роботи №1 Виконання лабораторної роботи №2	5 5
Модульна контрольна робота №1	5
Всього за змістовим модулем №1	15
ЗМІСТОВИЙ МОДУЛЬ №2 Витік небезпечного сигналу в навколишній радіо простір - 38 годин	

Виконання лабораторної роботи №3 Виконання лабораторної роботи №4 Модульна контрольна робота №2	5 5 5
Всього за змістовим модулем №2	15
ЗМІСТОВИЙ МОДУЛЬ №3 Фізична природа утворення каналу витоку в мережу електроживлення і в ланцюги заземлення» - 28 годин	
Виконання лабораторної роботи №5 Виконання лабораторної роботи №6 Модульна контрольна робота №3	5 5 5
Всього за змістовим модулем №3	15
ЗМІСТОВИЙ МОДУЛЬ №4 Утворення каналу витоку в лінії зв'язку - 36 годин	
Виконання лабораторної роботи №7	5
Виконання лабораторної роботи №8	5
Модульна контрольна робота №4	5
Всього за змістовим модулем №4	15
Додаткова частина	
Підготовка та захист реферату за індивідуальною темою	10
Участь у Днях студентської науки	10
Участь в науковій конференції за темою дисципліни	30
Участь в олімпіадах за темою дисципліни: - університетська - всеукраїнська	 20 30
Оформлення наочного стенда за індивідуальною темою	30
Для студентів денної форми навчання	
Вид навчальної роботи	Кількість балів *максимум*
Штрафна частина	
Пропуск одного заняття без поважної причини	-5
Здача звіту з лабораторних робіт пізніше узгодженого терміну	-5
НЕСВОЄЧАСНА ЗДАЧА ЗАЛІКУ	-20
ПІДСУМКОВА СЕМЕСТРОВА ОЦІНКА	**100**