ЖДТУ	**Міністерство освіти і науки України** **Житомирський державний технологічний університет**

Додаток 2

«ЗАТВЕРДЖУЮ»
Голова
Вченої ради факультету
інформаційно-комп'ютерних
технологій
(назва факультету)
_____
«_____» _____ 20___ р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ЗАХИСТ ІНФОРМАЦІЇ В ТК СИСТЕМАХ»

(назва навчальної дисципліни ВЕЛИКИМИ ЛІТЕРАМИ)

для студентів освітнього рівня «бакалавр»
(вказати: «бакалавр» АБО «магістр»)
спеціальності 172 «Телекомунікації та радіотехніка»
(шифр та назва спеціальності)
освітньо-професійна програма «Телекомунікації та радіотехніка»
(назва)
факультет інформаційно-комп'ютерних технологій
(назва)
кафедра біомедичної інженерії та телекомунікацій
(назва кафедри)

Робочу програму схвалено на засіданні
кафедри біомедичної інженерії та
телекомунікацій

протокол від «___» _____ 20__ р. № ___

Завідувач кафедри
біомедичної інженерії та телекомунікацій
(назва кафедри)
_____ _Нікітчук Т.М.
(підпис, ПІБ)

Розробник: старший викладач Полещук І.І.

Житомир
2018 – 2019 н.р.

ЖДТУ	Міністерство освіти і науки України Житомирський державний технологічний університет

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</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 – 5</td><td>Галузь знань:
17 «Електроніка та телекомунікація»</td><td colspan="2">Нормативна
(за вибором)</td></tr>
<tr><td>Модулів – 5</td><td rowspan="4">Спеціальність:
172 «Телекомунікації та радіотехніка»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів –5</td><td>2018-й</td><td>-й</td></tr>
<tr><td rowspan="3"></td><td colspan="2">Семестр</td></tr>
<tr><td>2-й</td><td>-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних –5
самостійної роботи студента - 10</td><td rowspan="10">Освітній рівень:
«бакалавр»»</td><td>24 год.</td><td>____ год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>24 год.</td><td>_____ год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>_ год.</td><td>____ год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>120 год.</td><td>____ год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання:
___год.</td></tr>
<tr><td colspan="2">Вид контролю:
екзамен</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Оволодіння студентами комплексом знань в області захисту інформації, системами й методами визначення захищеності програмних продуктів, пристроїв; телекомунікаційних та інформаційних мереж, їх складових та набуття на основі цих знань практичних навичок і теоретичних знань, необхідних для творчого підходу в питанні сучасного та в майбутньому оперативного захисту телекомунікаційних та інформаційних систем.

Оволодіння концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів; стратегією вибору систем виявлення атак, навичками роботи з пристроями безпеки в локальних і глобальних комп'ютерних мережах з метою використання їх, можливостей для покращення показників безпеки в них.

У результаті вивчення дисципліни студенти повинні:

- знати про джерела і способи дії загроз на об'єкти інформаційної

безпеки установ, про правові і нормативні акти, які визначають систему захисту інформації в державі; про документи, що визначають ступінь захищеності телекомунікаційних та інформаційних систем; методи аналізу надійності системи захисту інформації в телекомунікаційних та інформаційних системах; основні методи, технологію, принципи і правила захисту інформації, у тому числі персональних комп'ютерів, їх елементів і об'єктів комп'ютерних мереж;

- набути практичних навичок роботи з концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів; роботи із системами й методами визначення захищеності носіїв інформації; створення засобами стандартного програмного забезпечення елементів захисту інформації; формулювати завдання з питань захисту інформації, та формалізуючи їх, визначати шляхи їх вирішення.

3. Програма навчальної дисципліни

Тема № 1

Введення. Основні визначення

Тема № 2

Основні положення інформаційної безпеки

Тема № 3

Класифікація іноземної технічної розвідки. Можливості видів технічної розвідки

Технічні канали витоку інформації.

Тема № 4

Компоненти моделі безпеки інформації.

Тема № 5

Законодавчий рівень інформаційної безпеки.

Тема № 6

Адміністративний рівень рівень інформаційної безпеки.

Тема № 7

Організаційний рівень інформаційної безпеки.

Тема № 8.

Інженерно-технічний рівень інформаційної безпеки.

Тема № 9

Програмно-технічний захист інформаційних систем

4. Структура (тематичний план) навчальної дисципліни

Кредитні модулі	Змістовні модулі	Кількість годин			
		Всього	Лекції	Практичні	Самостійна робота
1	2	3	4	5	6
№ 1	Лекція 1..	6	2		4
	Лекція 2. Основні положення інформаційної безпеки	8	2		4
	Практичні заняття 1	4		2	2
	Разом змістовий модуль 1	**18**	**4**	**2**	**10**
№ 2	Лекція 3. Класифікація іноземної технічної розвідки. Можливості видів технічної розвідки Технічні канали витоку інформації	8	4		4
	Практичні заняття 2-6	20		10	10
	Разом змістовий модуль 2	***26***	***4***	***10***	***12***
№ 3	*Лекція 4.* Компоненти моделі безпеки інформації.	8	2		4
	Лекція 5. Законодавчий рівень інформаційної безпеки.	8	4		4
	Практичні заняття 7	4		2	2
	Разом змістовий модуль 3	**20**	**6**	**2**	**10**
№ 4	*Лекція 6.* Адміністративний рівень рівень інформаційної безпеки.	6	2		4
	Лекція 7. Організаційний рівень інформаційної безпеки.	6	2		4
	Практичні заняття 8	4		2	2
	Разом змістовий модуль 4	**16**	**4**	**2**	**10**
№ 5	*Лекція 8.* Інженерно-технічний рівень інформаційної безпеки.	12	4		4
	Лекція 9. Програмно-технічний захист інформаційних систем	10	2		4
	Практичні заняття 9-12			8	8
	Разом змістовний модуль 5	***22***	***6***	***8***	***8***
	ВСЬОГО	***106***	***24***	***24***	***50***

5. Теми семінарських (практичних, лабораторних) занять

Практичне заняття 1
Введення. Основні визначення.
Основні положення інформаційної безпеки

Практичне заняття 2
Технічні канали витоку інформації.
Структура, класифікація та основні характеристики
Елементарний електричний випромінювач
Елементарний магнітний випромінювач
Електромагнітні канали витоку інформації ТЗПІ
Електричні канали витоку інформації
Наведення електромагнітних випромінювань ТЗПІ
Параметричний канал витоку інформації.

Практичне заняття 3
Технічні канали витоку інформації при передачі її
по каналах святи
Електричні лінії зв'язку
Засоби передачі електричних сигналів
Канали витоку інформації за рахунок паразитних зв'язків
Небезпечні сигнали і їх джерела
Електричні канали витоку інформації
Контроль і прослуховування телефонних каналів зв'язку
Електромагнітні канали витоку інформації
Індукційний канал витоку інформації

Практичне заняття 4,5
Технічні канали витоку мовної інформації
Короткі відомості з акустики
звуковий поле
Лінійні характеристики звукового поля
Енергетичні характеристики звукового поля
плоска хвиля
сферична хвиля
Акустичні та електричні рівні
звукові сигнали
Маскування звукових сигналів
Зрозумілість і чіткість мови
Частотний діапазон і спектри
Звуковий поле в приміщенні
Звуковий фон в приміщенні
характеристики приміщення
Звукопоглинальні матеріали і конструкції

звукоізоляція приміщень
Акустичні канали витоку мовної інформації
мікрофони
спрямовані мікрофони
Провідні системи, портативні диктофони
і електронні стетоскопи
радіомікрофони
гідроакустичні датчики
СВЧ і ІК передавачі
Віброакустичні технічні канали витоку
мовної інформації
Акустоелектричні канали витоку мовної інформації
Акустоелектричні канали витоку мовної інформації
Оптико-електронний технічний канал витоку
мовної інформації
Параметричні технічні канали витоку
мовної інформації .

Практичне заняття 6
Технічні канали витоку видової інформації
Способи прихованого відеоспостереження і зйомки

Практичне заняття 7
Компоненти моделі безпеки інформації.
Законодавчий рівень інформаційної безпеки.

Практичне заняття 8
Компоненти моделі безпеки інформації.
Законодавчий рівень інформаційної безпеки.
Практичне заняття 8
Критий і ЗАХИСТ ІНФОРМАЦІЇ від витоку
Технічними каналами
Концепція і методи інженерно-технічного захисту інформації
Екранування електромагнітних хвиль
Електромагнітне екранування і розв'язують ланцюга
Придушення ємнісних паразитних зв'язків
Придушення індуктивних паразитних зв'язків
Екранування проводів і котушок індуктивності
екрановані приміщення.
Безпека оптоволоконних кабельних систем
Заземлення технічних засобів і придушення
інформаційних сигналів в ланцюгах заземлення
Фільтрація інформаційних сигналів

Основні відомості про помехоподавляющих фільтрах
Вибір типу фільтра
Просторове і лінійне зашумлення

Практичне заняття 9
Методи та засоби інженерного захисту
І технічної охорони об’єкту.
Категорії об'єктів захисту
Особливості задач охорони різних типів об'єктів
Загальні принципи забезпечення безпеки об'єктів
Система охоронно-тривожної сигналізації
Система контролю і управління доступом
телевізійні системи
Система пожежної сигналізації
Периметрова охорона

Практичне заняття 10
ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ
Основні поняття і класифікація загроз
Основні загрози доступності
Основні загрози цілісності
Основні загрози конфіденційності
Практичне заняття 11
ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
ІНФОРМАЦІЯ, ЩО ПІДЛЯГАЄ ЗАХИСТУ
ДІЇ, ЩО ПРИЗВОДЯТЬ ДО НЕПРАВОМІРНОГО ОВОЛОДІННЯ
КОНФІДЕНЦІЙНОЮ ІНФОРМАЦІЄЮ

Практичне заняття 12
Ітогове заняття.

Література для практичних занять
1. Технические средства и методы защиты информации:
Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков
Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО
«Издательство Машиностроение», 2009 – 508 с.

2. Лужецький В.А., Кожухівський А.Д., Войтович О.П.
Л 83 Основи інформаційної безпеки. Навчальний посібник. – Вінниця: ВНТУ,
2009. – 268 с.

6. Завдання для самостійної роботи

№	Назва теми	Кількість годин
1	1 Закон України “Про державну таємницю” від 21.01. 1994 р. №3855-XII. Закон України “Про захист інформації в автоматизованих системах” від 05.07. 1994 р. №80/94-ВР.	4
2	Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10. 1997 р. №1126.	4
3	1. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні поняття, – К.: Держстандарт України, 1996. – 8 с. 2. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. – К.: Держстандарт України, 1996. – 11 с. 3. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Терміни та визначення. – К.: Держстандарт України, 1996. – 16 с.	16
4	АТЕСТАЦІЯ ОБ'ЄКТІВ ІНФОРМАТИЗАЦІЇ 1. Заходи з виявлення й оцінки властивостей каналів витоку інформації. 2. Спеціальні перевірки. 3. Спеціальні обстеження. 4. Спеціальні дослідження акустичних і віброакустичних каналів. 5. Спеціальні дослідження технічних засобів і систем на можливість витоку інформації за рахунок побічних електромагнітних випромінювань і наводок.	**40**
РАЗОМ		**64**

7. Індивідуальні завдання

8. Методи контролю

При оцінюванні студентів приділяється перевага стандартизованим **методам контролю:**

- тестування (усне, письмове, комп'ютерне);
- структуровані письмові роботи;
- структурований контроль практичних навичок;
- контроль виконання практичної роботи;
- усне опитування;
- усна співбесіда.

Форми контролю:

Попередній (вхідний) контроль слугує засобом виявлення наявного рівня знань студентів для використання їх викладачем на практичному занятті як орієнтування у складності матеріалу. Проводиться з метою оцінки міцності знань та з метою визначення ступеня сприйняття нового навчального матеріалу.

Поточний контроль - контроль самостійної роботи студентів щодо вивчення навчальних матеріалів. Здійснюється на кожному практичному занятті відповідно до конкретних цілей теми з метою перевірити ступінь та якість засвоєння матеріалу, що вивчається. На всіх практичних заняттях застосовується об'єктивний контроль теоретичної підготовки та засвоєння практичних навичок із метою перевірки підготовленості студента до заняття. В процесі поточного контролю оцінюється самостійна робота студента щодо повноти виконання завдань, рівня засвоєння навчальних матеріалів, оволодіння практичними навичками аналітичної, дослідницької роботи та ін.

Рубіжний (тематичний) контроль засвоєння розділу (підрозділу) відбувається по завершенню вивчення блоку відповідних тем шляхом тестування та/або усної співбесіди та/або виконання структурованих завдань. Тематичний контроль є показником якості вивчення тем розділів дисципліни та засвоєння студентами практичних навичок, а також пов'язаних із цим пізнавальних, методичних, психологічних і організаційних якостей студентів. Проводиться на спеціально відведеному - підсумковому - занятті.

Проміжний контроль - полягає в оцінці засвоєння студентами навчального матеріалу на підставі виконання ним певних видів робіт на практичних (семінарських) заняттях за певний період. Проводиться у формі семестрового заліку на останньому практичному (семінарському) занятті в семестрі.

Підсумковий контроль здійснює контролюючу функцію, проводиться з метою оцінки результатів навчання на певному освітньо-кваліфікаційному рівні або на окремих його завершених етапах. Проводиться у формі заліку, диференційованого заліку або іспиту з метою встановлення змісту знань студентів за обсягом, якістю та глибиною, а також вміннями застосувати їх у практичній діяльності. Під час підсумкового контролю враховуються результати складання здачі усіх видів навчальної роботи згідно із структурою робочої програми.

ПРИМІТКА: Кафедра визначає форми контролю відповідно до навчального плану з дисципліни.

9. Схема нарахування балів

10. Рекомендована література

Основна література

1. Лужецький В. А., Кожухівський А. Д., Войтович О. П. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ Вінницький національний технічний університет 2008 -279 с
2. Авраменко В.Ф., Брудний Г.О., Жлобін С.І., Лазарев Г.П., Дорошко В.О. Правові основи охорони інформації. – К.: ТОВ „Поліграф Консалтинг”, 2003. – 173 с.
3. Анин Б. Защита компьютерной информации. – СПб. БХВ-Санкт-Питербург, 2000. – 384 с.
4. Бабак В.П., Корченко О.Г. Інформаційна безпека та сучасні мережеві технології.. – К.: «МК-Пресс», 2003. – 248 с.
5. Бармен Скотт. Разработка правил информационной безопасности. Пер. с англ. – М.: «Вільямс», 2002. – 208 с.
6. Белов Е.Б. и др. Основы информационной безопасности. Учебное пособие для вузов . – М.: Горячая линия–Телеком, 2006. – 544 с.
7. Вертузаєв М.С., Юрченко О.М. Захист інформації в комп’ютерних системах від несанкціонованого доступу. Навч. посібник / За ред. С.Г. Лаптева. – К.: Вид-во Європ. ун-ту, 2001. – 321 с.
8. Галатенко В.А. Основы информационной безопасности. // http://www.intuit.ru/department/security/secbasics/
9. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері використання комп’ютерних технологій. Навч. посібник / За заг. ред. доктора юридичних наук, професора Р.А. Калюжного. – Запоріжжя: ГУ „ЗІДМУ”, 2002. – 292 с.
10. Домарев В.В. Безопасность информационных технологий. Методология создания ситем защиты. – К.: ООО «ТИД «ДС», 2001. – 688 с.
11. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях – М.: КУДИЦ-ОБРАЗ, 2001. – 346 с.
12. Касперски К. Техника сетевых атак. – М.: Солон-Р, 2001. – 524 с.
13. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекомуникационных системах. – К.: «МК-Пресс», 2005. – 288 с.
14. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб: БХВ-Петербург, 2003. – 752 с.
15. Лужецький В.А., Войтович О.П., Дудатьєв А.В. Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 240 с.
16. Лужецький В.А., Войтович О.П., Дудатьєв А.В. Захист персональних даних. Навчальний посібник. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 240 с.
17. Лукацкий А.В. Обнаружение атак. – СПб: БХВ-Петербург, 2001. – 224 с.
18. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 280 с.

19. Медведев Н.Г., Москалюк Д.В. Аспекты информационной безопасности виртуальных частных сетей. Учебное пособие. – К.: Изд-во Европ. ун-та, 2002. – 95 с.
20. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.
21. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях // Под ред. В. Ф. Шаньгина. – М.: Радио и связь, 2001. – 376 с.
22. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.
23. Смит Р.Э. Аутентификация: от паролей до открытых ключей. – М.: «Вильямс», 2002. – 432 с.
24. Столингс В. Криптография и защита сетей: принципы и практика, 2-е изд. : Пер. с англ. – М.: «Вильямс», 2001. – 672 с.
25. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії. Навчальний посібник. – Вінниця: ВДТУ, 2003. – 143 с.
26. Чмора А.Л. Современная прикладная криптография. – М.: Гелиус АРВ, 2001. – 244 с.
27. Ярочкин В.И. Информационная безопасность. Учебное пособие. – М.: Междунар. отношения, 2000. – 400 с.

Допоміжна література

1. Закон України "Про інформацію" від 02.10. 1992 р. №2657-XII.
2. Закон України "Про науково-технічну інформацію" від 25.06. 1993 р. №3322-XII.
3. Закон України "Про державну таємницю" від 21.01. 1994 р. №3855-XII.
4. Закон України "Про захист інформації в автоматизованих системах" від 05.07. 1994 р. №80/94-ВР.
5. Закон України "Про Концепцію Національної програми інформатизації" від 04.02. 1998 р. №75/98-ВР.
6. Закон України "Про ліцензування певних видів господарської діяльності" від 01.06. 2000 р. №1775-III.
7. Закон України "Про стандартизацію" від 17.05. 2001 р. №2408-III.
8. Закон України "Про авторське право і суміжні права" від 23.12. 1993 р. №3792-XII (в редакції закону України від 11.07. 2001 р. №2627-III, з подальшими змінами та доповненнями).
9. Закон України "Про електронні документи та електронний документообіг" від 22.05. 2003 р. №851-IV.
10. Закон України "Про електронний підпис" від 22.05. 2003 р. № 852-IV.
11. Закон України "Про охорону прав на промислові зразки" від 15.12. 1993 р. №3688-XII (із змінами і доповненнями станом на 01.01. 2004р.).

12. Закон України “Про охорону прав на знаки для товарів і послуг” від 15.12. 1993 р. №3689-XII (із змінами і доповненнями станом на 01.01. 2004 р.).
13. Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10. 1997 р. №1126.
14. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні поняття, – К.: Держстандарт України, 1996. – 8 с.
15. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. – К.: Держстандарт України, 1996. – 11 с.
16. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Терміни та визначення. – К.: Держстандарт України, 1996. – 16 с.
17. Правила обов’язкової сертифікації засобів обчислювальної техніки (Затв. наказом Держстандарту України від 25.06. 1997 р. №366).
18. Правила обов’язкової сертифікації технічних засобів охоронної та охоронно-пожежної сигналізації (Затв. наказом Держстандарту України від 10.04. 1997 р. №191).
19. Аграновский А.В., Пузыренко А.Н. Компьютерная стеганография: Теория и практика. - МК-Пресс, 2006. - 283 с.
20. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. - М.: Гелиос АРВ, 2001. - 480 с.
21. Шнайер, Брюс. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003. – 368 с.