Міністерство освіти і науки України
Національний університет водного господарства та природокористування
Навчально-науковий інститут автоматики, кібернетики та обчислювальної техніки
Кафедра обчислювальної техніки

04-04-09

"ЗАТВЕРДЖУЮ"
Проректор з науково-педагогічної, методичної та виховної роботи
_____ Лагоднюк О.А.
"__"_____ 2018 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Program of the Discipline

Організація захисту інформації в комп'ютерних системах

Organization of information security in computer systems

спеціальність	**123 "Комп'ютерна інженерія"**
specialty	**123 Computer Engineering**

Рівне – 2018

Робоча програма "Організація захисту інформації в комп'ютерних системах " для здобувачів вищої освіти другого (магістерського) рівня, які навчаються за спеціальністю 123 "Комп'ютерна інженерія". Рівне: НУВГП, 2018. – 19 с.

Розробник: Назарук Віталій Дмитрович, ст. викладач кафедри обчислювальної техніки, к.т.н

Робочу програму схвалено на засіданні кафедри обчислювальної тех-ніки. Протокол від " 07 " вересня 2018 року № 1.
Завідувач кафедри _____ Б.Б. Круліковський

Схвалено науково-методичною комісією за спеціальністю 123 "Комп'ютерна інженерія". Протокол від "10" вересня 2018 року № 1
Голова науково-методичної комісії _____ М.Т. Соломко

ВСТУП

Програма нормативної навчальної дисципліни " Організація захисту інформації в комп'ютерних системах " складена на підставі вимог навчального плану для здобувачів вищої освіти другого (магістерського рівня). Предметом вивчення навчальної дисципліни є формування у студентів теоретичних знань і розуміння принципів побудови систем технічного захисту інформації в комп'ютерних системах, а також практичних навичок роботи по розробці моделей загроз та моделей порушників інформації. Опанування основних положень зазначеного курсу передбачає наявність міждисциплінарних зв'язків таких дисциплін, як "Інформатика", "Теорія інформації", "Архітектура комп'ютера", «Захист інформації в комп'ютерних системах». На матеріалі даної дисципліни може ґрунтуватись вивчення наступних професійно спрямованих дисциплін: "Технологія проектування комп'ютерних систем", "Комп'ютерні системи".

Анотація

Навчальний курс призначений для вивчення організації захисту інформації в комп'ютерних системах, в якому викладено загальні підходи до розробки моделей загроз та порушників, формування на їх основі заходів захисту інформації. Подано методику створення комплексних систем захисту інформації в автоматизованих системах. Надано порядок використання нормативних документів в галузі технічного захисту інформації та рекомендації щодо порядку функціонування служб захисту інформації в автоматизованих системах.

Ключові слова: модель порушника, модель загроз, автоматизована система, критерії загроз, комплексна система захисту інформації.

Abstract

The training course is designed to study the organization of

information security in computer systems, which outlines general approaches to the development of threats and offenders, and the formation of information security measures on their basis. The method of creation of complex systems of information protection in automated systems is given. The procedure for using normative documents in the field of technical protection of information and recommendations on the operation of information security services in automated systems is given.

Key words: model of the perpetrator, model of threats, automated system, criterion of threats, complex system of information protection.

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</td><td>заочна форма</td></tr>
<tr><td>Кількість кредитів – 6</td><td>Галузь знань
12 Інформаційні технології</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – 2</td><td rowspan="3">Спеціальність
123 "Комп’ютерна інженерія"</td><td colspan="2">Рік підготовки</td></tr>
<tr><td rowspan="2">Змістових модулів – 2</td><td>5-й</td><td>5-й</td></tr>
<tr><td rowspan="3">Спеціалізація
"Комп’ютерні системи
та компоненти"</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 180</td><td>10-й</td><td>10-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="2">Тижневих годин для денної фор-</td><td rowspan="2">Рівень вищої світи:
2 магістерський</td><td>22 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
</table>

ми навчання: аудиторних – 6 самостійної роботи –7		36 год.	10 год.
		Самостійна робота	
		98год.	138 год.
		Індивідуальні завдання:	
		24	24
		Форма контролю:	
		іспит	

Примітка. Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання –32/ 68%

для заочної форми навчання – 10/ 90 %.

2. Мета та завдання навчальної дисципліни

Метою викладання дисципліни є набуття теоретичних знань та практичних навичок побудови систем технічного та криптографічного захисту інформації на основі розроблених моделей загроз.

Завданням дисципліни є:

- формування системного підходу до дослідження систем технічного та криптографічного захисту інформації в комп'ютерних системах;
- набуття навиків розроблення моделі загроз та моделі порушника інформаційно-комп'ютерних систем;
- отримання знань порядку застосування існуючих та перспективних технологій захисту інформації.

В результаті вивчення дисципліни студенти повинні

знати:

- види загроз для інформації в комп'ютерних системах, їх класифікацію та наслідки реалізації;
- теоретичні основи техніічних каналів витоку інформації, способи їх локалізації на об'єктах інформаційної діяльності;
- принципи роботи сучасних симетричних та асиметричних криптоалгоритмів;
- порядок формування електронного цифрового підпису.

вміти:

- виконувати моніторинг процесів функціонування комп'ютерних

мереж та інформаційно-телекомунікаційних систем в умовах реалізації загроз різних класів та впливів зовнішніх дестабілізуючих факторів з метою зменшення їх впливу на процеси обміну даними;
- застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності;
- забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановлено політики безпеки.

3. Програма навчальної дисципліни
Модуль 1.

Змістовий модуль 1.Вимоги міжнародних та вітчизняних законодавчих та нормативних документів із захисту інформації та кібербезпеки.

Тема № 1. Правовий статус інформації. Поняття інформації з обмеженим доступом. Вимоги перших міжнародних стандартів із захисту інформації.

Тема № 2. Основні положення міжнародного стандарту ISO/IEC 15408.Тема № 3. Міжнародний стандарт ISO/IEC 27002 «Інформаційні технології – Методики безпеки – Практичні правила управління безпекою інформації».

Тема № 4. Законодавча база із захисту інформації в Україні. Основні положення законів України «Про захист інформації в інформаційно-телекомунікаційних системах» «Про кібербезпеку», Постанови КМУ «Концепція технічного захисту інформації в Україні»

Тема № 5: Нормативна база із захисту інформації в Україні. Основні вимоги нормативних документів «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності обробльованої інформації від несанкціонованого доступ», «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

Тема № 6. Вимоги із захисту інформації в багатомашинних багатокористувацьких комплексах. Вимоги із захисту службової інформації від несанкціонованого доступу в автоматизованих системах класу 2.

Тема № 7. Вимоги із захисту інформації в багатомашинних багатокористувацьких комплексах. Вимоги до захисту інформації вебсторінки від несанкціонованого доступу

Модуль 2.

Змістовий модуль 2. Створення та супроводження комплексних систем захисту інформації

Тема № 8. Розроблення технічного завдання на створення комплексної системи захисту інформації. Порядок проведення робіт зі створення комплексних систем захисту. Вимоги до комплексної системи захисту інформації та політика безпеки

Тема № 9. Створення комплексної системи захисту інформації (частина 1). Розроблення політики безпеки. Аналіз ризиків. Визначення вимог до заходів, методів і засобів захисту.

Тема № 10. Створення комплексної системи захисту інформації (частина 2). Розроблення проекту комплексної системи захисту інформації. Введення комплексної системи захисту інформації в дію та оцінювання захищеності інформації в інформаційно-телекомунікаційних системах.

Тема № 11. Супроводження комплексної системи захисту інформації. Положення про службу захисту інформації в АС Завдання та функції служби захисту інформації. Організація робіт служби захисту інформації та їх фінансування.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин									
	денна форма					заочна форма				
	всього	у тому числі				всього	у тому числі			
		лекції	лаборат.	індівід..	с. р.с.		лекції	лаборат.	індівід..	с. р.с.
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
Модуль 1										
Змістовий модуль 1. Вимоги міжнародних та вітчизняних законодавчих та нормативних документів із захисту інформації та кібербезпеки.										
Тема № 1. Правовий статус інформації. Поняття інформації з обмеженим доступом. Вимоги перших міжнародних стандартів із захисту інформації.	14	2			12	14				14
Тема № 2. Основні положення міжнародного стандарту ISO/IEC 15408.	14	2	2		10	14				14
Тема № 3. Міжнародний стандарт ISO/IEC 27002 «Інформаційні технології – Методики безпеки – Практичні правила управління безпекою інформації».	14	2	2		10	14				14
Тема № 4. Законодавча база із захисту	14	2	2		10	14				14

інформації в Україні.										
Тема № 5: Нормативна база із захисту інформації в Україні.	14	2	2		10	14	2	2		10
Тема № 6. Вимоги із захисту інформації в багатомашинних багатокористувацьких комплексах. Вимоги із захисту службової інформації від несанкціонованого доступу в автоматизованих системах класу 2.	14	2	2		10	14	2	2		10
Тема № 7. Вимоги із захисту інформації в багатомашинних багатокористувацьких комплексах. Вимоги до захисту інформації веб-сторінки від несанкціонованого доступу.	14	2	4		8	14		2		12
Разом за змістовим модулем 1	98	14	14		70	98	4	6		88
Модуль 2										
Змістовий модуль 2. Створення та супроводження комплексних систем захисту інформації										
Тема № 8. Розроблення технічного завдання на створення комплексної системи захисту інформації. Порядок ство-	14	2	4		8	14	2	2		10

рення і впровадження КСЗІ.										
Тема № 9. Створення комплексної системи захисту інформації (частина 1).	14	2	6		6	14	2	2		10
Тема № 10. Створення комплексної системи захисту інформації (частина 2).	15	2	6		7	15				15
Тема № 11. Супроводження комплексної системи захисту інформації.	15	2	6		7	15				15
Разом за змістовим модулем 2	58	8	22		46	58	4	6		50
Усього годин	156	22	36		98	156	8	10		138
Курсовий проект				24					24	
Разом	180	22	36	24	98	180	8	10	24	138

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Лабораторна робота № 1. Застосування термінів, визначених нормативними документами ТЗІ для підготовки документів при створенні КСЗІ	2	
2	Лабораторна робота № 2. Підготовка Загальних положень, та розділу 1 «Положення про службу захисту інформації	2	
3	Лабораторна робота № 3. Підготовка розділу 2 «Положення про службу захисту інформації».	2	
4	Лабораторна робота № 4. Підготовка розділу 3 «Положення про службу захисту інформації».	2	
5	Лабораторна робота № 5. Підготовка розділів 4 – 5 «Положення про службу захисту інформації».	2	2
6	Лабораторна робота № 6. Підготовка розділів 1,2 «Плану захисту інформації в автоматизованій системі».	2	2
7	Лабораторна робота № 7 Підготовка розділу 3 «Плану захисту інформації в автоматизованій системі».	2	2
8	Лабораторна робота № 8 Підготовка підрозділу 4.1. розділу 4. «Плану захисту інформації в автоматизованій системі».	2	2
9	Лабораторна робота № 9 Підготовка підрозділу 4.2. розділу 4. «Плану захисту інформації в автоматизованій системі».	2	2
10	Лабораторна робота № 10 Підготовка розділу 5 «Плану захисту інформації в автомати-	2	

	зованій системі»		
11	Лабораторна робота № 11 Підготовка «Акту категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці».	2	
12	Лабораторна робота № 12 Підготовка «Акту обстеження на об'єкті інформаційної діяльності».	2	
13	Лабораторна робота № 13 Здійснення класифікації автоматизованої системи та вибір функціональних профілів захищеності.	2	
14	Лабораторна робота № 14 Опис функціональних профілів захищеності. Частина 1.	2	
15	Лабораторна робота № 15 Опис функціональних профілів захищеності. Частина 2.	2	
16	Лабораторна робота № 16 Опис функціональних профілів захищеності. Частина 3.	2	
17	Лабораторна робота № 17 Опис функціональних профілів захищеності. Частина 4.	2	
18	Лабораторна робота № 18 Опис функціональних профілів захищеності. Частина 5.	2	
	Разом	36	8

6. Самостійна робота

За навчальним планом на самостійну роботу відводиться 122 години для студентів денної форми навчання та 162 години для студентів заочної форми навчання.

Самостійна робота студента включає наступні види робіт:

- самостійне опрацювання лекційного матеріалу з кожної теми;
- підготовка до виконання лабораторних робіт;
- обробка результатів досліджень, оформлення звітів, підготовка та захист лабораторних робіт;
- підготовка до модульних контрольних робіт (тестування);
- виконання індивідуального навчально-дослідного завдання (курсової роботи);

- підготовка до підсумкового контролю (іспит).

6.1 Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Правовий статус інформації. Поняття інформації з обмеженим доступом. Вимоги перших міжнародних стандартів із захисту інформації.	12	14
2	Основні положення міжнародного стандарту ISO/IEC 15408.	10	14
3	Міжнародний стандарт ISO/IEC 27002 «Інформаційні технології – Методики безпеки – Практичні правила управління безпекою інформації».	10	14
4	Законодавча база із захисту інформації в Україні.	10	14
5	Нормативна база із захисту інформації в Україні.	10	10
6	Вимоги із захисту інформації в багатомашинних багатокористувацьких комплексах. Вимоги із захисту службової інформації від несанкціонованого доступу в автоматизованих системах класу 2.	10	10
7	Вимоги із захисту інформації в багатомашинних багатокористувацьких комплексах. Вимоги до захисту інформації веб-сторінки від несанкціонованого доступу.	8	12
8	Розроблення технічного завдання на створення комплексної системи захисту інформації. Порядок створення і впровадження КСЗІ.	8	10
9	Створення комплексної системи захисту інформації (частина 1).	6	10
10	Створення комплексної системи захисту інфо-	7	15

	рмації (частина 2).		
11	Супроводження комплексної системи захисту інформації.	7	15
	Разом	98	138

7. Індивідуальне навчально-дослідне завдання

Індивідуальним навчально-дослідним завданням передбачено розробку та написання курсової роботи з предмету «Організація захисту інформації в комп'ютерних системах». Обсяг курсової роботи до 50 сторінок пояснювальної записки. Тематика курсових робіт та методика виконання викладені у відповідних методичних рекомендаціях. Час, розрахований на курсове проектування становить 24 години самостійної роботи. До структури курсової роботи повинні увійти всі розділи технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі класу 1.

8. Методи навчання

Лекційні заняття проводяться з використанням проектора, переносних комп'ютерів викладача та студентів Завдання лабораторних робіт передбачають, в тому числі, виконання завдань учбово-дослідного характеру з частково невизначеними умовами.

9. Методи контролю

Для поточного контролю знань студентів з навчальної дисципліни використовуються такі методи:

- на лекційних заняттях проводиться контроль присутності студентів та контроль якості конспектів лекцій;
- на лабораторних заняттях проводиться контроль готовності до заняття шляхом тестового експрес-опитування, а також шляхом захисту звітів з лабораторної роботи у вигляді співбесіди;
- контроль самостійної роботи проводиться у вигляді співбесіди на задану тему;
- оцінка модульних контрольних робіт (тестування);
- підсумковий контроль проводиться в кінці семестра у вигляді іспиту.

Усі форми контролю включено до 100-бальної шкали оціню-

вання.

Оцінювання результатів поточної роботи (завдань, що виконуються на лабораторних заняттях, результати самостійної роботи студентів) проводиться за такими критеріями:

Лабораторні роботи (у % від кількості балів, виділених на завдання із заокругленням до цілого числа):

0 % – завдання не виконано;

40% – завдання виконано частково та містить суттєві помилки методичного або розрахункового характеру;

60% – завдання виконано повністю, але містить суттєві помилки у розрахунках або в методиці;

80% – завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки (розмірності, висновки, оформлення тощо);

100% – завдання виконано правильно, вчасно і без зауважень.

10. Розподіл балів, що отримують студенти

Поточне тестування та самостійна робота											Підсумковий тест (іспит)	Сума
Змістовий модуль 1							Змістовий модуль 2				40	100
T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}		
4	4	4	4	4	4	4	8	8	8	8		

T_1, T_2 ... T_{18} – теми змістових модулів.

За виконання курсової роботи

Пояснювальна записка	Захист роботи	Сума
60	40	100

Шкала оцінювання

Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою	
	для екзамену, курсового проекту (роботи)	для заліку
90-100	відмінно	зараховано
82-89	добре	
74-81		
64-73	задовільно	
60-63		
35-59	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

11. Методичне забезпечення

1. Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни «Організація захисту інформації» для здобувачів вищої освіти другого (магістерського) рівня галузі знань 12 «Інформаційні технології» спеціальності 123 «Комп'ютерна інженерія» денної та заочної форм навчання /Назарук В.Д. - Рівне: НУВГП. 2018. - 31 с. Електронний ресурс. Режим доступу http://ep3.nuwm.edu.ua/id/eprint /7328/.

2. Методичні вказівки до виконання курсового проекту з навчальної дисципліни «Організація захисту інформації» для здобувачів вищої освіти другого (магістерського) рівня галузі знань 12 «Інформаційні технології» спеціальності 123 «Комп'ютерна інженерія» денної та заочної форм навчання /Назарук В.Д. - Рівне: НУВГП. 2018. - 21 с. Електронний ресурс. Режим доступу http://ep3.nuwm.edu.ua/id/eprint /7329/.

12. Рекомендована література

Базова

1. Грайворонський М.В., Новіков О.М Безпека інформаційно-комунікаційних систем Київ: БХВ, 2009, 596 с.
2. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
3. Домарев В. В. Безопасность информационных технологий: Системный подход: - К.: ООО "ТИД ДС", 2004. – 992с.
4. Конев И. Р., Беляев А. В. Информационная безопасность предприятия.- СПб.: БХВ - Петербург, 2003, 752с.: ил.

Допоміжна

1. Белов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А. Основы информационной безопасности. Учебное пособие для вузов - М.: Горячая линия - Телеком, 2006. - 544 с: ил.

2. Биячуев Т. А. / под ред. Л. Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.

3. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Логос, 2001. - 264 с : ил.

4. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. 452с., ил.

5. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. - М: Горячая линия-Телеком, 2004. -280 с. ил.

6. Малюк А. А., Пазизин С. В., Погожин Н.С. Введение в защиту информации в автоматизированных Системах. - М.: Горячая линия-Телеком, 2001. - 148 с: ил.

7. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. – СПб.: Питер, 2002.- 848 с.: ил.

8. Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997.- 368с.:ил.

13. Інформаційні ресурси

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» 80/94-ВР,. Режим доступу: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

2. Закон України Про основні засади забезпечення кібербезпеки України від 05.10.2017. Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-19

3. Постанова Кабінету міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» 1126-97-п. Режим доступу: http://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF

4. Нормативний документ з технічного захисту інформації «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» (зі зміною № 1). Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407

5. Нормативний документ з технічного захисту інформації « Критерії оцінки захищеності інформації в комп'ютерних системах від

несанкціонованого доступу». Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740&cat_id=89734

6. Нормативний документ з технічного захисту інформації « Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу “2”». Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740&cat_id=89734

7. Нормативний документ з технічного захисту інформації « Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу». Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740&cat_id=89734