Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра інженерії програмного забезпечення (№ 603)

ЗАТВЕРДЖУЮ

Керівник проектної групи/

_____ І.Б. Туркін
(підпис) (ініціали та прізвище)

«30» 08 2019 р.

РОБОЧА ПРОГРАМА *ОБОВ'ЯЗКОВОЇ* НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека програм та даних
(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр та найменування галузі знань)

Спеціальність: 121 «Інженерія програмного забезпечення»
(код та найменування спеціальності)

Освітня програма: «Інженерія програмного забезпечення»
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2019 рік

2

Робоча програма «Безпека програм та даних» для студентів за спеціальністю: 121 «Інженерія програмного забезпечення» освітньою програмою «Інженерія програмного забезпечення»

«20» 04 2019 р, – 13 с.

Розробник: Дем'яненко В.А., ст.викладач . кафедри №603,
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри інженерії програмного забезпечення
(назва кафедри)

Протокол № 1 від «30» 08 2019 р.

Завідувач кафедри д-р техн. наук., проф. І.Б. Туркін
(науковий ступінь і вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показника</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни (денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 4</td><td rowspan="10">Галузь знань
12 «Інформаційні технології»
(шифр і найменування)

Спеціальність
121 «Інженерія програмного забезпечення»
(код і найменування)

Освітня програма
«Інженерія програмного забезпечення»
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td>Цикл професійної підготовки (2.1. Дисципліни загально-професійної підготовки)</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 3</td><td>2019/2020</td></tr>
<tr><td>Індивідуальне завдання _____
(назва)</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 56/120</td><td>_7_-й</td></tr>
<tr><td>Лекції*</td></tr>
<tr><td rowspan="5">Кількість тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 3,5</td><td>_32_ години</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>___ годин</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>_24_ годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>_64_ годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: 56/64.

*Аудиторне навантаження може бути зменшене або збільшене на одну годину залежно від розкладу занять.

2. Мета та завдання навчальної дисципліни

2.1. Метою викладання навчальної дисципліни “ Безпека програм та даних ” є вивчення потенційних загроз безпеки інформації, будування систем захисту інформації, а також вивчення методів захисту інформації від несанкціонованого доступу (НСД) та принципи побудови систем контролю та захисту інформації (СКЗІ). Мета досягається за рахунок сполучення таких форм навчання, як лекції та лабораторні роботи, а також самостійної роботи студентів.

2.2 Основними завданнями дисципліни “ Безпека програм та даних ” є сформувати знання та отримати вміння виконання комплексу завдань, найважливішими серед яких є виконання процедур аутентифікації, авторизації та аудиту, дотримання конфіденційності, доступності та цілісності даних.

2.3 Згідно з вимогами освітньо-професійної програми студенти повинні:

знати:

- Властивості інформації;
- Фізичне подання інформації та процеси її обробки;
- Криптографічні моделі та методи захисту інформації;
- Концептуальні основи проектування захисту інформації.

вміти:

- обмежувати доступ до інформації;
- виконувати контроль доступу до апаратури;
- створювати системи захисту інформації

мати навички:

- Створення систем контролю та захисту інформації.

Міждисциплінарні зв’язки – дисципліні передують курси: «Основи програмування», «Математичний аналіз», «Теорія ймовірностей та емпіричні методи програмної інженерії», «Об’єктно-орієнтоване програмування»

3. Програма навчальної дисципліни

Модуль 1.

Змістовий модуль 1. Задачі та призначення курсу

Основні питання:

1. Задачі та призначення курсу. Термінологія. Властивості та види інформації. Інформація захисту: види та форми подання інформації. Машинне подання інформації. Фізичне подання інформації та процеси її обробки. Об’єкти захисту: Класифікація об’єктів захисту інформації. Організація проектування АСОД. Умови та режими експлуатації АСОД

2. Загрози. Потенційні загрози безпеки інформації. Випадкові загрози. Навмисні загрози.

3. Методи захисту. Огляд методів захисту інформації. Програмні. Апаратні. Контроль та доступ. Обмеження доступу. Контроль доступу до апаратури.

Розмежування та контроль доступу до інформації. Ідентифікація. Розподілення привілей на доступ. Ідентифікація та встановлення дійсності об’єкту (суб’єкту).

4. Криптографія. Криптографічне перетворення інформації. Огляд та класифікація методів шифрування інформації.

Змістовий модуль 2. Криптографічне перетворення інформації

Симетричні криптосистеми. Задачі методу перетворення. Коди. Шифри. Шифр VERNAN Системи з відкритим ключем. Криптографія по приватному ключу. Механізми шифрування по секретному ключу. Криптографія по загальному ключу. Багатопользовательські криптографічні методи. Вимоги до криптосистем. Обмеження на криптографію. Криптографічні атаки Підпис та хешування.Засоби формування цифрового підпису інформації, що передається. Побудова хєш-функцій. Аналіз методів захисту. Вибір засобів захисту інформації в трактах передачі даних.

Модуль 2.

Змістовий модуль 3. Сучасні методи захисту інформації

Сучасні методи безпеки. Аналіз сучасних методів оцінки захищеності інформації. Принциповий підхід до оцінки рівня безпеки інформації від навмисного НСД

4. Структура навчальної дисциплін

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1 *Задачі та призначення курсу*					
Тема 1. *Задачі та призначення курсу. Термінологія. Властивості та види інформації*	6	2	-	-	4
Тема 2. *Види та форми подання інформації. Машинне подання інформації. Фізичне подання інформації та процеси її обробки*	6	2	-	-	4
Тема 3. *Класифікація об'єктів захисту інформації. Організація проектування АСОД.*	6	2	-		4
Тема 4. *Потенційні загрози безпеки інформації. Випадкові загрози. Навмисні загрози*	6	2	-	1	3
Тема 5. *Огляд методів захисту інформації*	6	2	-		4
Тема 6. *Обмеження доступу. Контроль доступу до апаратури. Розмежування та контроль доступу до інформації*	6	2	-	1	3
Тема 7. *Розподілення привілей на доступ. Ідентифікація та встановлення дійсності об'єкту (суб'єкт)*	6	2	-	2	2
Тема 8. *Криптографічне перетворення інформації. Огляд та класифікація методів шифрування інформації*	6	2	-	2	2
Разом за змістовним модулем 1	48	16	-	6	26
Усього годин	**48**	**16**	**-**	**6**	**26**

Змістовний модуль 2. *Криптографічне перетворення інформації*					
Тема 9. *Вибір методу перетворення. Коди. Шифри. Шифр VERNAN.*	6	2	-	2	2
Тема 10. *Криптографія за приватним ключем. Механізми шифрування по таємному ключу.*	6	2	-	2	2
Тема 11. *Криптографія по загальному ключу. Багатопользовательські криптографічні методи.*	6	2		2	2
Тема 12. *Обмеження на криптографію. Криптографічні атаки.*	6	2		2	2
Тема 13. *Засоби формування цифрового підпису інформації, що передається*	6	2		2	2
Тема 14. *Вибір засобів захисту інформації в трактах передачі даних Аналіз сучасних методів оцінки захищеності інформації. Принциповий підхід до оцінки рівня безпеки інформації від навмисного НСД*	6	2		2	2
Модульний контроль	5				5
Разом за змістовним модулем 2	41	12	-	12	17
Усього годин	**89**	**28**	**-**	**18**	**43**
Модуль 2					
Змістовний модуль 3 *Сучасні методи захисту інформації*					
Тема 15. *Сучасні методи захисту інформації WinCrypt API*	16	4	-	6	6
Модульний контроль	5				5
Разом за змістовним модулем 3	21	4	-	12	17
Контрольний захід	10				10
Усього годин	**120**	**32**	**-**	**24**	**64**

5. Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Шифри перестановок	1
2	Шифри заміни	1
3	Криптоаналіз за допомогою частотних характеристик	1
4	Шифрування гамуванням	1
5	Шифрування алгоритмом DES	1
6	Шифрування методом Вернама	1
7	Блочні шифри	1
8	Шифрування IDEA	2
9	Системи з відкритим ключем RSA	2
10	Шифрування Полига-Хеллмана	2
11	Шифрування Єль-Гамаля	2
12	Перевірка відповідності ключа	1
13	Хешування	1
14	Електронний підпис та сигнатура	1
15	Сучасні методи захисту інформації WinCrypt API	6
	Разом	24

6. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Поняття криптологія, криптография, криптоаналіз.	1
2	Поняття алфавіт, текст, ключ.	1
3	Поняття криптоаналіз. Виды криптоаналіза.	1
4	Поняття стенографія.	1
5	Поняття шифрування, дешифрування, ключ.	1
6	Поняття криптосистеми. Види криптосистем.	1
7	Вимоги до криптосистем.	1
8	Поняття електронного підпису та сігнатури.	1
9	Поняття криптостійкости.	1
10	Симетричні криптосистеми. Види криптосистем.	1
11	Симетричні криптосистемы. Підстановки.	1
12	Симетричні криптосистемы. Перестановки.	1
13	Симетричні криптосистемы. Гаммируваннґ.	1
14	Симетричні криптосистемы. Блокові шифри.	1
15	Датчики ПВЧ. Особливості застосування.	1
16	Поняття криптосистеми з відкритим ключем.	1
17	Особливості алгоритму RSA.	1
18	Особливості криптосистеми Эль-Гамаля.	1
19	Особенности криптосистем на основі элліптичних	1

	рівнянь.	
20	Электронний підпис. Особливості захисту.	1
21	Цифрова сігнатура. Особливості захисту	1
22	Хэш-функції. Особливості захисту	1
23	Службы та механізми захисту	1
24	Поняття ідентифікації та аутентифікації.	1
25	Типи та механізми захисту	1
26	Управління доступом.	1
27	Забезпечення конфіденційності повідомлень і даних.	1
28	Забезпечення цілістності даних.	1
29	Реєстрація та спостереження.	1
30	Реєстрація дій користувача.	1
31	Метод парольного захисту та його модифікайії.	1
32	Система управління ключами.	1
33	Засоби аутентифікації та контролю доступа.	1
34	Засоби захисту інформации в ИС.	1
35	Класифікація хеш-функцій.	1
36	Безключові хеш-функціи.	1
37	Цифрові підписи.	1
38	Класифікація цифрових підписів.	1
39	Цифрова підпис з добавленням.	1
40	Цифрова підпись з відновленням	1
41	Механізми невідказності	1
42	Загальні вимоги до систем захисту інформації (СЗІ).	1
43	Організаційні вимоги до систем захисту інформації (СЗІ).	1
44	Вимоги до підсистем зіхисту інформації (СЗІ).	1
45	Вимоги до технічного забезпечення систем захисту інформації (СЗІ).	1
46	Вимоги до ПЗ систем захисту інформації (СЗІ).	1
47	Вимоги до застосування засобів, методів та способів захисту.	1
48	Вимоги до документування СЗІ.	1
49	Вимоги до складу проектної та експлуатаційної документації.	1
50	Загальні функціональні задачі, що повинна вирішувати СЗІ.	1
51	Виконання індивідуального завдання	4
52	Підготовка до контрольних заходів	10
	Разом	64

7. Методи навчання

1. За джерелами придбання знань – словесні: лекція (вступна, традиційна, проблемна, з помилками), бесіда (евристична), диспут, дискусія, робота з друкованими та інтернет-джерелами; наочні: ілюстрація, спостереження; практичні: вправа, лабораторна робота.
2. За характером пізнавальної діяльності тих, хто навчається – інформаційно-репродуктивний, репродуктивний, проблемне викладання, частково-пошуковий.
3. За логікою пізнання – індуктивний, дедуктивний, аналогій, вивідних знань.
4. Методи перевірки й оцінки знань, умінь, навичок: спостереження, усне опитування, контрольні роботи, програмований контроль, тестування (традиційне та машинне).

8. Методи контролю

Опитування на лекціях. Виконання і захист лабораторних робіт. Модульні контрольні роботи.

Форма підсумкового контролю успішності навчання: іспит (письмово) у 7 семестрі

9. Критерії оцінювання та розподіл балів, які отримують студенти

9.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…1	8	0…8
Виконання і захист лабораторних (практичних) робіт	2...5	4	8...20
Змістовний модуль 2			
Робота на лекціях	0…1	6	0…6
Виконання і захист лабораторних (практичних) робіт	2...3	6	12...18
Модульний контроль	10…20	1	10…20
Змістовний модуль 3			
Робота на лекціях	0…1	2	0…2
Виконання і захист лабораторних (практичних) робіт	3...6	1	3...6
Модульний контроль	10…20	1	10…20
Усього за семестр			**60…100**

Семестровий контроль (іспит) проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту/заліку складається з двох теоретичних питань (кожне питання 50 балів)

9.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки: властивості інформації; фізичне подання інформації та процеси її обробки; криптографічні моделі та методи захисту інформації; концептуальні основи проектування захисту інформації

Необхідний обсяг вмінь для одержання позитивної оцінки: обмежувати доступ до інформації;виконувати контроль доступу до апаратури;створювати системи захисту інформації

9.3. Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь.

Добре (75-89). Твердо знати мінімум, здати тестування та поза аудиторну самостійну роботу.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх.

Шкала оцінювання: національна та ECTS

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ECTS</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, курсового проекту (роботи), практики</td><td>для заліку</td></tr>
<tr><td>90 – 100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>83 – 89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>75 – 82</td><td>C</td></tr>
<tr><td>68 – 74</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60 – 67</td><td>E</td></tr>
<tr><td>1 – 59</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного складання</td></tr>
</table>

10.Методичне забезпечення

1. Розроблений лекційний курс. Student:\\2016-2017\6 факультет\4 курс\Безопасность программ и данных\ CRYPTOBE.DOC
2. Розроблено та надруковано учбовий посібник Student:\\2016-2017\6 факультет\4 курс\Безопасность программ и данных\ Безопасность программ и данніх - Демьяненко.docx
3. Розроблений комплекс питань для опитування студентів. Student:\\2016-2017\6 факультет\4 курс\Безопасность программ и данных\ Билеты по ММЗИ.doc
4. Розроблено електронний посібник Student:\\2016-2017\6 факультет\4 курс\Безопасность программ и данных\ WinCryptAPI\index.html
5. Лабораторні роботи. Student:\\2016-2017\6 факультет\4 курс\Безопасность программ и данных\LAB\
6. Дібрані матеріали для самостійної роботи студентів. Student:\\2016-2017\6 факультет\4 курс\Безопасность программ и данных\Inet\

11. Рекомендована література

Базова

1. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си (Брюс Шнайер). Издательство: Триумф, 2013 -815с.
2. Цифровая стеганография. Издательство: Солон-Пресс, 2016 – 272с.
3. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика. 1997 – 368с.
4. Либерти Джесс. С++. Энциклопедия пользователя: Пер. с англ./Джесс Либерти – К.: Издательство «ДиаСофт», 2000 –584с.
5. Труды института инженеров по электротехнике и радиоэлектронике (ТИИЭР). Малый тематический выпуск «Защита информации»: пер. с англ., Том 76, №5, Май 1998.
6. Домарев В.В. Защита информации и безопасность комптютерных систем. – К.: Издательство «ДиаСофт», 1999. – 480 с.

Допоміжна

1. Дж. Л. Месси. Введение в современную криптологию. // ТИИЭР, т.76, №5, Май 88 – М, Мир, 1988, с.24-42.
2. У. Диффи. Первые десять лет криптографии с открытым ключом. // ТИИЭР, т.76, №5, Май 88 – М, Мир, 1988, с.54-74.
3. А. В. Спесивцев и др. Защита информации в персональных компьютерах. – М., Радио и связь. 1992, с.140-149.
4. В. Жельников. Криптография от папируса до компьютера. – М., ABF, 1996.

12. Інформаційні ресурси

1. http://pidruchniki.ws/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi
2. http://cryptography.ru/
3. http://algolist.manual.ru/defence/intro.php