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

кафедра Систем управління літальних апаратів (№ 301)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ О.В. Гавриленко
(підпис) (ініціали та прізвище)

«____» _____ 2021 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇДИСЦИПЛІНИ

«Захист інформації в системах управління»
(назва навчальної дисципліни)

Галузі знань: 15 «Автоматизація та приладобудування»,

Спеціальність: 151 «Автоматизація та комп'ютерно інтегровані технології»,

Освітні програми: «Інженерія мобільних додатків

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2021 рік

Розробник:
к.т.н., доцент Немшилов Ю.О., доцент кафедри Систем управління літальних апаратів

«27» серпня 2021 р. _____
(підпис)

Робочу програму розглянуто на засіданні кафедри Систем управління_літальних апаратів
Протокол № 1 від “ 27 ” серпня 2021 р.

Завідувач кафедри 301 к.т.н., доцент _____ К. Ю. Дергачов
(підпис) (прізвище та ініціали)

1. Опис навчальної дисципліни

<table>
<tr><td colspan="2">Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td colspan="4">Денна форма навчання</td></tr>
<tr><td colspan="2" rowspan="2">Кількість кредитів - 4</td><td rowspan="3">Галузь знань
15 «Автоматизація та приладобудування»,</td><td>Дисципліна професійної підготовки</td></tr>
<tr><td rowspan="2">Навчальний рік:</td></tr>
<tr><td colspan="2">Модулів – 3</td></tr>
<tr><td colspan="2">Змістових модулів – 3</td><td rowspan="2">Спеціальність:
151 «Автоматизація та комп’ютерно інтегровані технології»</td><td>2021/2022</td></tr>
<tr><td colspan="2">Загальна кількість годин денна: кількість годин аудиторних занять / загальна кількість годин – 48/72</td><td>Семестр</td></tr>
<tr><td colspan="2" rowspan="2">Кількість тижневих годин для денної форми навчання
Семестр 6</td><td rowspan="4">Освітні програми: Інженерія мобільних додатків, Комп’ютерні системи технічного зору</td><td>6</td></tr>
<tr><td>Лекції[1)]</td></tr>
<tr><td>Аудиторних – 3 год.</td><td>Самост. роботи – 4,5 год.</td><td>16</td></tr>
<tr><td colspan="2"></td><td>Практичні[1)]</td></tr>
<tr><td colspan="2"></td><td rowspan="2">16</td></tr>
<tr><td colspan="2"></td><td>Лабораторні[1)]</td></tr>
<tr><td colspan="2"></td><td rowspan="4">Рівень вищої освіти: перший (бакалаврський)</td><td>16</td></tr>
<tr><td colspan="2"></td><td>Самостійна робота</td></tr>
<tr><td colspan="2"></td><td>72</td></tr>
<tr><td colspan="2"></td><td>Вид контролю</td></tr>
<tr><td colspan="2"></td><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить для денної форми навчання – 48/72.

Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета – ознайомити з принципами побудови та використання програмних та програмно апаратніх засобів для захисту програмного забезпечення та іншої інформації в комп'ютерних системах.

Завдання – надати основні відомості з принципів побудови систем захисту інформації та методів протидії спробам несанкціонованого доступу до неї з боку сторонніх осіб, привласнення привілей тощо.

Загальні компетентності (ЗК)

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК2. Здатність застосовувати знання у практичних ситуаціях.
ЗК3. Здатність спілкуватися іноземною мовою.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК8.Здатність приймати обґрунтовані рішення.
ЗК11.Здатність працювати автономно.

Фахові компетентності спеціальності (ФК)

ФК1. Вміння використовувати базові знання основних національних, європейських та міжнародних нормативно-правових актів в галузі систем автоматизації із застосуванням мобільних додатків з метою постійного вдосконалювання своєї професійної діяльності.
ФК2. Вміння використовувати досягнення науки і техніки в професійній діяльності, аргументувати вибір методів розв'язування спеціалізованих завдань з аналізу та синтезу систем автоматизації.
ФК3. Здатність реалізовувати та використовувати апаратні та програмно-алгоритмічні засоби щодо збільшення точності та надійності систем управління.
ФК6. Вміння аналізувати системи автоматизації з мобільними пристроями, формувати архітектуру систем автоматичного управління, виділяти підсистеми, що є складовими загальної системи та взаємозв'язки поміж ними.
ФК7. Вміння визначати склад випробувального обладнання, необхідного для проведення експериментів по визначенню характеристик і параметрів систем управління і автоматизації.
ФК10. Вміння оцінювати техніко-економічну ефективність проектування систем управління і автоматизації із застосуванням мобільних додатків.

У результаті вивчення навчальної дисципліни студент повинен

знати:

– об'єкти програмного забезпечення, на яки можливи атакі з боку комп'ютерних хакерів, та методи здійснення несанкціонованого доступу до інформації;

– принципи функціонування вбудованих засобів захисту комп'ютерних систем (BIOS) та шляхи протидії спробам їх взлому;

– принципи функціонування систем захисту, призначення привілей, сберігання паролів та автентіфікація користувачів в операційних системах;

вміти:

– виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи несанкціонованого доступу виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи несанкціонованого доступу;

– здійснити організаційни та програмні заходи щодо підвищення рівня безпеки зберігання інформації;

мати уявлення:

– мати уявлення про основні напрямки та перспективи розвитку методів і засобів захисту інформації та управління правами використання інформаційних ресурсів при передачі конфіденційної інформації по каналах зв'язку, встановлення автентичності переданих повідомлень, зберігання інформації (документів, баз даних), встановленні прихованої службової інформації.

Програмні результати навчання

ПРН2. Використовувати базові знання основних національних, європейських та міжнародних нормативно-правових актів у галузі систем автоматизації з метою постійного вдосконалювання своєї професійної діяльності.

ПРН3. Використовувати досягнення науки і техніки в професійній діяльності, аргументувати вибір методів розв'язування спеціалізованих завдань з аналізу та синтезу систем автоматизації з мобільними пристроями.

ПРН4. Застосовувати сучасні технології автоматизації проектування та конструювання інформаційно-управляючих систем у галузі автоматизації, вміти створювати апаратно-програмні засоби стосовно збільшення точності, надійності функціонування систем управління із мобільними додатками.

ПРН5. Розробляти технічні завдання на проектування систем управління із мобільними пристроями та засобів технологічного оснащення, вибирати обладнання й технологічне оснащення.

ПРН7. Аналізувати та створювати архітектуру систем автоматичного і автоматизованого управління, виділяти підсистеми та об'єкти, що є складовими системи, та взаємозв'язки поміж ними.

ПРН10. Оцінювати техніко-економічну ефективність проектування систем управління і автоматизації із застосуванням мобільних додатків.

Пререквізіти:

Вища математика. Основи моделювання. Математичні основи цифрових систем. Методи обчислення та програмування на ЕОМ.

Кореквізіти:

ООП програм для мобіільних систем (КР).
Мікроконтролери в системах управління.
Теорія автоматичного управління.
Системи управління літальними апаратами.
Теорія цифрових систем управління.

3. Програма навчальної дисципліни

Змістовий модуль 1.

Тема 1. Вступ до навчальноїдисципліни. Предмет вивчення і задачі дисципліни «Захист інформації в СУ». Завдання. Основні поняття. Сучасні інформаційні загрози.

Тема 2. Характеристика технічніх каналів та просочування інформації.

Структура, класифікація і основні характеристики технічних каналів просочування інфо рмації. Автоматизація виявлення складових тестового сигналу.

Концепція і методи інженерно-технічного захисту інформації

Модульний контроль.

Змістовий модуль 2.

Тема 3. Основні поняття та алгоритми прикладної криптографії.

Введення в криптографію. Шифри заміни.

Основні терміни, використовувані в криптографії

Тема 4. Системи числення. Цифрове кодування інформації.

Змішані системи числення Коди, що не базуються на системах числення

Тема 5. Теоретичні основи завадостійкого кодування

Теоретичні основи завадостійкого кодування

Класифікація завадостійких кодів

Тема 6. Потокові шифри і генератори псевдовипадкових чисел.

Принципи використання генераторів псевдовипадкових чисел при потоковому шифруванні.

Модульний контроль.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	денна форма				
	усього	у тому числі			
		лекц.	практ.	лаб	сам.р.
1	2	3	4	5	7
Змістовий модуль 1					
Тема 1. Вступ до навчальноїдисципліни. Предмет вивчення і задачі дисципліни «Захист інформації в СУ».	15	2	2	2	9
Тема 2.Характеристика технічніх каналів та просочування інформації	44	6	5	6	27
Модульний контроль	1		1		
Змістовий модуль 2					
Тема 3. Основні поняття та алгоритми прикладної криптографії.	15	2	2	2	9
Тема 4. Системи числення. Цифрове кодування інформації.	13	2		2	9
Тема 5. Теоретичні основи завадостійкого кодування	16	2	3	2	9
Тема 6. Потокові шифри і генератори псевдовипадкових чисел.	15	2	2	2	9
Модульний контроль	1		1		
РАЗОМ	120	16	16	16	72

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	Не заплановано	
2		

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Дослідження процесу шифрування за допомогою простої заміни і грат Кардано.	2
2	Дослідження процесу обчислення ключів у блоковому шифрі S - DES .	2
3	Дослідження процесу расшифрования повідомлень за допомогою спрощеного S - DES	2
4	Дослідження потокового шифрування повідомлень в системах, що самосинхронизуються	2
5	Дослідження потокового шифрування повідомлень в системах, що самосинхронизуються, з генераторами Фиббоначи	2
6	Дослідження процесу шифрування Эль-Гамаля	2
7	Дослідження процесу побудови прихованого каналу на основі схеми Эль-	2

	Гамаля	
8	Дослідження процесу побудови прихованого каналу на основі схеми Густава-Симмонсона	2
	Разом	16

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Дослідження процесу шифрування повідомлення за допомогою Таблиці Виженера	2
2	Дослідження процесу шифрування повідомлень за допомогою спрощеного S - DES	2
3	Дослідження потокового шифрування повідомлень в синхронних системах	2
4	Дослідження потокового шифрування повідомлень в системах, що синхронізуються, з генераторами Фиббоначи	2
5	Дослідження процесу ассиметричного шифрування без передачі ключа	2
6	Дослідження процесу шифрування RSA	2
7	Дослідження процесу шифрування Рабинера	2
8	Дослідження процесу побудови електронного підпису на основі алгоритму RSA	2
	Разом	16

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Тема 1. Вступ до навчальноїдисципліни. Предмет вивчення і задачі дисципліни «Захист інформації в СУ».	9
2	Тема 2.Характеристика технічніх каналів та просочування інформації	27
3	Тема 3. Основні поняття та алгоритми прикладної криптографії.	9
4	Тема 4. Системи числення. Цифрове кодування інформації.	9
5	Тема 5. Теоретичні основи завадостійкого кодування	9
6	Тема 6. Потокові шифри і генератори псевдовипадкових чисел.	9
	Разом	72

10. Методи навчання

Словесно – наочні: лекції, практичні: лабораторні та практичні роботи, індивідуальні консультації (при необхідності), самостійна робота студентів за матеріалами, опублікованими кафедрою (методичні посібники).

11. Методи контролю

Поточний контроль - відповідно до змістових модулів і тем у вигляді письмового опитування; усного опитування; тестування.

Семестровий контроль – у вигляді письмового іспиту.

Критерії оцінювання та розподіл балів, які отримують студенти

Розподіл балів, які отримують студенти за семестр

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…1	4	0…4
Виконання і захист лабораторних робіт	0…6	4	0...24
Виконання і захист практичних робіт	0...5	4	0...20
Модульний контроль	0…2	1	0…2
Змістовний модуль 2			
Робота на лекціях	0…1	4	0…4
Виконання і захист лабораторних робіт	0…6	4	0 …24
Виконання і захист практичних робіт	0...5	4	0...20
Модульний контроль	0…2	1	0…2
Усього за семестр			**0…100**

Білет для іспиту складається з теоретичних та практичних запитань. Наприклад.

Теоретичні питання (40 балів):
Традиційні симетричні криптосистеми.
Практичні завдання (30 балів):
Шифрування повідомлень за допомогою класичних методів перестановки та підстановки:
Лабораторні завдання (30 балів):
За допомогою криптосистеми RSA згенерувати відкритий та таємний ключи (розробіть код програми) для повідомлення

Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

- національні стандарти щодо інформації;
- об’єкти програмного забезпчення, на яки можливи атакі з боку комп'ютерних хакерів, та методи здійснення несанкціонованого доступу до інформації;
- принципи функціонування вбудованих засобів захисту комп'ютерних систем(BIOS) та шляхи протидії спробам їх взлому;
- принципи функціонування систем захисту, призначення привілей, сберігання паролів та автентіфікація користувачів в операційних системах;
- програмного забезпечення, на яки можливи атакі з боку комп'ютерних хакерів, та методи здійснення несанкціонованого доступу до інформації.

Необхідний обсяг вмінь для одержання позитивної оцінки:

виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи несанкціонованого доступу;

виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи несанкціонованого доступу.

Критерії оцінювання роботи студента протягом семестру

1. Відмінно (90÷100 балів) виставляється студенту:

Який твердо знає: базові поняття і принципи, що відносяться до дисципліни «Захист інформації в системах управління» індивідуальне завдання, виконав усі модульні завдання з оцінкою «відмінно», має тверді практичні навички з апаратурою. Вільно користується навчальною та науково-технічною літературою з питань дисципліни. Вміє логічно і чітко скласти свою відповідь, розв'язати практичне та лабораторне завдання.

Зменшення кількості балів в межах оцінки можливе при неточних формулюваннях у відповідях на додаткові запитання, які були поставлені перед ним.

2. Добре (75÷89 балів) виставляється студенту:

Який має достатньо глибокі знання з теоретичної частини дисципліни. Захистив всі практичні, лабораторні завдання та індивідуальне завдання, виконав усі модульні завдання з оцінкою «добре», має практичні навички роботи зі схемотехніки. Правильно розв'язує практичні завдання, його відповіді не є чіткими.

Зменшення кількості балів в межах оцінки можливе при неповнихвідповідях на теоретичні або практичні запитання.

3. Задовільно (60÷74 бали) виставляється студенту:

Який слабо володіє теоретичним матеріалом, має мінімум знань та умінь, допускає помилки у вирішенні практичних завдань.Захистив всі практичні, лабораторні завдання та індивідуальне завдання, виконав усі модульні завдання, має не впевнені практичні навички роботи з технікою.Зменшення кількості балів в межах оцінки можливе за неточні та неповні відповіді на теоретичні та практичні запитання.

Шкала оцінювання: національна та ECTS

Сума балів	Оцінка за традиційною шкалою	
	Іспит	Залік
90 – 100	Відмінно	Зараховано
75 - 80	Добре	
60 - 74	Задовільно	
0 -59	Незадовільно	Незараховано

14. Методичне забезпечення

1. Конспект лекцій з дисципліни «Захист інформації в СУ».
2. Методичні вказівки і завдання до виконання лабораторних робіт.
3. Методичні вказівки і завдання до виконання розрахункових робіт.
4. НМКД в електронному вигляді розміщене на сервері каф. 301

15. Рекомендована література

Базова

1. Захист інформації в автоматизованих системах управління [Текст]: навч. посібник/ Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с
2. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2017. – 72 с.
3. Захарченко М.В., Йона Л.Г., Щербіна Ю.В., Онацький О.В. Розвинення криптології та її місце в сучасному суспільстві : Навч. посібник. - Одеса: ОНАЗ ім.. О.С. Попова, 2016. - 80 с.
4. Домарєв В. В., Швець В. А., Шестакова В. В. Організаційне забезпечення захисту інформації з обмеженим доступом: Навчальний посібник. / Національний авіаційний університет; МОН. – К.: НАУ, 2006. – 108 с.
5. За редакцією Горбенко І.Д. Горбенко Ю.І. «Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації». Електронна версія. Монографія. Харків. Форт. 2016 , 902с.

Допоміжна

1. Лідовский В.В. Теория информации. – М.: Наука. –2003. – 112с.
2. Малюк А.А., Пазизин В.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М,: Телеком, 2001 – 148 с.
3. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. – М.: ГЛТ, 2016. – 586 с

15. Інформаційні ресурси

Сайт кафедри 301: **k301.khai.edu**.

1. ua/box/2/26.shtml
2. / - Методы и средства защиты информации
3. / - Журнал «Открытые Системы»
4. / - Журнал «HackZone»
5. / Международные стандарты безопасности ISO