ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПОВІТРЯНИХ СИЛ ІМ. ІВАНА КОЖЕДУБА

ІНСТИТУТ ЦИВІЛЬНОЇ АВІАЦІЇ

Кафедра
інформаційних технологій

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Рівень вищої освіти	перший (бакалаврський)
Ступінь вищої освіти	Бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	121 Інженерія програмного забезпечення

Шифр ВБ3.1

Х а р к і в
2 0 1 9

Розроблено та внесено:

Інститутом цивільної авіації Харківського національного університету Повітряних Сил імені Івана Кожедуба.

Розробники програми: Сєвєрінов Олександр Васильович – доцент кафедри інформаційних технологій, кандидат технічних наук, доцент.

Ухвалено на засіданні вченої ради
Харківського національного університету Повітряних Сил
імені Івана Кожедуба
Протокол від "___" _____ 201_ року, № __

ВСТУП

Програма вивчення навчальної дисципліни "Безпека програм та даних" відноситься до циклу дисциплін професійної та практичної підготовки й складена відповідно до освітньої програми підготовки фахівців.

Рівень вищої освіти перший (бакалаврський)
Ступінь вищої освіти Бакалавр
Галузь знань 12 Інформаційні технології
Спеціальність 121 Інженерія програмного забезпечення

Предметом вивчення навчальної дисципліни "Безпека програм та даних" є вивчення основних методів, механізмів, алгоритмів та протоколів криптографічного захисту інформації в інформаційних системах.

Науковою основою дисципліни є положення, які пов’язані з криптографічним захистом інформації в інформаційних системах.

Міждисциплінарні зв’язки: для успішного вивчення дисципліни "Безпека програм та даних" необхідні базові знання, отримані студентами при освоєнні ними дисципліни "Інформатика та обчислювальна техніка", "Дискретна математика", "Теорія ймовірностей". Навчальна дисципліна "Безпека програм та даних" є інструментальною основою для вивчення дисциплін професійної підготовки, курсових та атестаційних робіт. Вона забезпечує наступні дисципліни: "Комп’ютерні мережі", "Розробка мобільних застосувань", "Корпоративні інформаційні системи", дипломного проектування.

Програма навчальної дисципліни складається з таких змістових модулів:

1. Змістовний модуль 1.1. Модель захисту інформації.
2. Змістовний модуль 1.2. Криптографічні перетворення для забезпечення конфіденційності інформації.
3. Змістовний модуль 2.1. Генерація ключових даних.
4. Змістовний модуль 2.2. Основи теорії автентичності.
5. Змістовний модуль 2.3. Протоколи безпеки бездротових мереж

1. Загальна мета навчальної дисципліни

Мета викладання навчальної дисципліни "Безпека програм та даних" полягає в засвоєнні необхідних знань з опанування основних методів, механізмів, протоколів, алгоритмів та стандартів криптографічного захисту інформації, формування у студента навичок в галузі використання засобів криптографічного перетворення для вирішення практичних задач захисту даних та забезпечення інформаційної безпеки, що дозволить в подальшому випускнику успішно працювати в обраній сфері.

2. Компетентності, які набуваються під час засвоєння навчальної дисципліни

1. ЗК-1 Здатність до абстрактного мислення, аналізу й синтезу.
2. ЗК-2 Здатність застосовувати знання в практичних ситуаціях.
3. ЗК-5 Навички використання інформаційних і комунікаційних технологій
4. ФК-6 Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки.
5. ФК-8 Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв’язання завдань інженерії програмного забезпечення.

3. Запланований результат навчання

Згідно з вимогами освітньої програми визначені та сформульовані наступні результати навчання студентів:

1. РН-4 Знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення.
2. РН-18 Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних
3. РН-21 Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем

4. Зміст навчальної дисципліни

На засвоєння навчальної дисципліни відводиться 150 годин/ 5,0 кредитів ЄКТС.

Блок змістовних модулів 1.

Змістовний модуль 1.1. Модель захисту інформації

Функції систем захисту інформації. Основні поняття інформаційної безпеки. Історія криптографії. Нормативно-правова база захисту інформації.

Погрози інформаційної безпеки в комп'ютерних системах. Класифікація погроз інформаційної безпеки. Загрози інформаційної безпеки

бездротових системах. Загрози безпеці у мережах.

Структурна схема захищеної інформаційної системи. Основні показники якості шифрів. Класифікація криптосистем за стійкістю.

Змістовний модуль 1.2. Криптографічні перетворення для забезпечення конфіденційності інформації

Класифікація криптоперетворень. Класичні симетричні методи шифрування. Поняття блокового шифру. Потокові шифри. Сучасні алгоритми потокового шифрування.

Методологія побудови симетричних криптосистем. Сучасні блокові алгоритми симетричного шифрування. Вимоги до блокових симетричних шифрів.

Принципи побудови криптосистем з відкритими ключами. Криптосистеми з відкритими ключами на основі алгоритмів рюкзака. Криптосистема RSA.

Сучасні алгоритми спрямованого шифрування. Асиметричні криптосистеми на базі еліптичних кривих.

Блок змістовних модулів 2.

Змістовний модуль 2.1. Генерація ключових даних.

Історія розвитку методів генерації випадкових послідовностей. Вимоги до генераторів ключів. Основні алгоритми генерування ключових даних.

Контроль ефективності функціонування генераторів ключових послідовностей. Методика тестування NIST STS. Стандарт FIPS-140-1.

Змістовний модуль 2.2. Основи теорії автентичності

Основи теорії автентичності. Схема моделі взаємної недовіри і взаємного захисту.

Теорія автентичності Сімонсона. Методи автентифікації, що використовують паролі та PIN-коди. Методи автентифікації в класі симетричних шифрів.

Основні визначення та вимоги до функцій ґешування. Основні алгоритми ґешування.

Визначення електронного цифрового підпису. Порядок формування та перевірки підпису. Класифікація та вимоги до цифрових підписів

Змістовний модуль 2.3. Протоколи безпеки бездротових мереж

Основи бездротової передачі інформації Wi-Fi. Механізми шифрування у стандарті Wi-Fi. Механізми автентифікації стандарту 802.11. Стандарт 802.1x/EAP. Вразливості протоколів безпеки в мережах Wi-Fi.

Протоколи безпеки бездротових мереж GSM. Автентифікація абонента в мережі GSM A3. Механізм шифрування A5. Механізм шифрування KASUMI. Вразливості алгоритмів шифрування A5.

5. Рекомендована література

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків: ХНУРЕ. Форт, 2012, 878 с.
2. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Л.Я. Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с.
3. Ю.І. Горбенко, І.Д. Горбенко. «Інфраструктури відкритих ключів. Електроний цифровий підпис. Теорія та практика»: Монографія. – Х.: Вид. «Форт»,. - 2010. – 608 с.
4. Задірака В. Комп'ютерна криптологія. Підручник. К, 2002 , 504 с.
5. Устенко І.В. Системи захисту інформації: навч. Посіб. – Миколаїв: НУК, 2006. – 68 с.
6. Основи інформаційної безпеки: навч. посіб. / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович ; Вінниц. нац. техн. ун-т. - Вінниця : ВНТУ, 2013. - 220 с.
7. Кавун С.В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 2008. - 352 с.
8. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с.
9. Закон України «Про інформацію».
10. Закон України «Про захист інформації в інформаційно–телекомунікаційних системах».
11. Закон України «Про електронний цифровий підпис».
12. Закон України «Про електронні документи та електронний документообіг».
13. Закон України «Про основні засади забезпечення кібербезпеки України».
14. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 № 1229.
15. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу
16. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу
17. http://metod.kart.edu.ua/
18. www.rsasecurity.com
19. www.nist.gov
20. www.eprint.iacr.org
21. www.citeseer.ist.psu.edu
22. www.ansi.org
23. www.cryptography.org
24. 7.www.iso.org
25. www.cryptography.com
26. www.financialcryptography.com
27. http://world.std.com/~franl/crypto.html
28. www.cryptonessie.org

6. Види та форми контролю успішності навчання

6.1. Для зворотного зв’язку за якістю та успішністю навчання в навчальній дисципліні використовуються такі види контролю: вхідний, поточний, модульний (рубіжний), семестровий (підсумковий), підсумковий.

Вхідний контроль проводиться перед вивченням навчальної дисципліни з метою визначення рівня підготовки студентів (слухачів, студентів) з навчальних дисциплін, які забезпечували вивчення цієї навчальної дисципліни або загальноосвітнього рівня підготовки у формі письмового тесту. За результатами вхідного контролю розробляються заходи з надання індивідуальної допомоги студентам (слухачам, студентам).

Поточний контроль проводиться на всіх видах навчальних занять та проводиться у формі усного опитування або письмового експрес-контролю (летючки) під час проведення навчальних занять, а також у формі комп’ютерного (або письмового) тестування. Результати поточного контролю є основною інформацією під час проведення модульного контролю і при визначенні підсумкової оцінки.

Модульний (рубіжний) контроль проводиться після вивчення логічно завершеної частини (змістового модуля) програми навчальної дисципліни у формі усного опитування, контрольної роботи, тестування тощо. Результати модульного (рубіжного) контролю враховуються при визначенні підсумкової екзаменаційної оцінки з даної навчальної дисципліни.

Семестровий (підсумковий) контроль проводиться відповідно до навчального плану у вигляді екзамену. Форма проведення семестрового контролю (усна, письмова, комбінована, тестування тощо), зміст і структура контрольних завдань, екзаменаційних білетів та критерії оцінювання визначаються робочою програмою навчальної дисципліни. Екзамен проводиться шляхом усної відповіді за білетом та вирішення практичного завдання.

6.2. Оцінювання результатів підсумкового контролю навчальних досягнень студентів здійснюється за 100-бальною шкалою, за шкалою ЄКТС та національною шкалою згідно табл. 1.

Таблиця 1 - Шкала оцінювання: 100-бальна, ECTS та національна

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 - 100	A	відмінно	зараховано
80 - 89	B	добре	
65 - 79	C		
55 - 64	D	задовільно	
50 - 54	E		
35 - 49	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1 - 34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

Обов’язковою умовою задовільної атестації під час семестрового контролю є відсутність заборгованостей з практичних занять, семестрового індивідуального завдання (контрольної роботи). В разі наявності у студента

академічних заборгованостей за дисципліну студент до екзамену не допускається.

Студенти, які не виконали індивідуальні завдання або мають інші заборгованості з поважних причин, ліквідують академічну заборгованість у термін, встановлений начальником університету. Повторне перескладання екзамену допускається не більше двох разів. Друге перескладання екзамену у студентів приймає комісія, яка створюється начальником кафедри.

7. Засоби діагностики успішності навчання

Засобом проведення вхідного контролю з навчальної дисципліни є тест. Засобами проведення поточного контролю з навчальної дисципліни експрес-летючки та переліки питань для усного опитування в методичній розробці для проведення заняття. Засобами проведення модульного (рубіжного) контролю є контрольна робота (тест, індивідуальне завдання та ін.). Засобом проведення семестрового (підсумкового) контролю є фонд контрольних завдань (фонд екзаменаційних білетів, електронний тест, тощо).

Завідувач кафедри інформаційних технологій
кандидат технічних наук доцент

І.ІЛЬЇНА

"___" _____ 201__ року