Затверджено Вченою Радою ОНУ
імені І.І. Мечникова
від “20”грудня 20 16 р. № 4

Одеський національний університет імені І.І. Мечникова
Факультет математики, фізики та інформаційних технологій
Кафедра математичного забезпечення комп’ютерних систем

“ЗАТВЕРДЖУЮ”
Проректор з науково-педагогічної роботи
_____
“____” _____ 20___ р.

НАВЧАЛЬНА ПРОГРАМА ДИСЦИПЛІНИ

ОК25 «Технології захисту інформації»
(назва навчальної дисципліни)

Рівень вищої освіти _____бакалавр_____

Спеціальність _____126 – Інформаційні системи та технології_____
(код і назва спеціальності (тей)

2019

Розробник:
Шпінарева І.М., к.ф.-м. н., доцент

Навчальна програма затверджена на засіданні кафедри математичного забезпечення комп'ютерних систем

Протокол № 1 від. "30" 08 2019 р.

Завідувач кафедри _____ (Є.В. Малахов)
(підпис) (прізвище та ініціали)

Обговорено та рекомендовано до затвердження навчально-методичною комісією (НМК) з ІТ факультету МФІТ

Протокол № 1 від. "23" 09 2019 р.

Голова НМК _____ (О.В. Савастру)
(підпис) (прізвище та ініціали)

Вступ

Навчальна програма дисципліни «Технології захисту інформації» складена відповідно до освітньо-професійної програми підготовки бакалаврів спеціальності 126 – Інформаційні системи та технології (версія **2019** р.).

Предметом дисципліни є технології, методи та стандарти захисту інформації.

Місце дисципліни і значення в структурі навчального процесу.

Вивчення курсу та виконання лабораторних робіт базується на знанні програмування, складу та структури комп'ютерних систем та мереж, засобів та методів проектування комп'ютерних та інформаційних систем, що викладаються у дисциплінах «Інженерія програмного забезпечення», «Системний аналіз», «Проектування інформаційних» та «Економіка і організація інформаційного бізнесу».

Програма навчальної дисципліни складається з таких змістових модулів:

1. Основні положення теорії інформаційної безпеки та захисту інформації. Основи криптографії.
2. Методи захисту в комп'ютерних системах.
3. Механізми і політики розмежування прав доступу в ОС.

1. Мета та завдання навчальної дисципліни

Метою вивчення дисципліни є формування комплексу знань, вмінь в галузі теорії захисту інформації, в використані методів та засобів забезпечення інформаційної безпеки та здобуття навичок у практичному використанні криптографічних методів у створенні захищених комп'ютерних систем.

Задачі дисципліни:

– отримати знання основних аспектів проблеми забезпечення безпеки інформації;

– отримати знання методів та засобів забезпечення безпеки комп'ютерної інформації для вирішення практичних завдань в інформаційних системах, які виникають при зберіганні, обробці та передаванні інформації;

– оволодіти знаннями побудови систем захисту з використанням методів традиційної криптографії;

– використовувати методи контролю цілісності і автентичності інформації, у тому числі протоколи аутентифікації та електронного підпису.

Процес вивчення дисципліни спрямований на формування елементів наступних **компетентностей**:

а) загальних (ЗК):

КЗ 6. Здатність до пошуку, оброблення та узагальнення інформації з різних джерел.

б) фахових загальних (КФЗ):

КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу

даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.

в) спеціальних фахових (КФС):

КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

КС 14. Здатність формувати нові конкурентоспроможні ідеї й реалізовувати їх у проектах (стартапах).

Програмні результати навчання:

ПРН 4. Проводити системний аналіз об'єктів проектування та обґрунтовувати вибір структури, алгоритмів та способів передачі інформації в інформаційних системах та технологіях.

ПРН 6. Демонструвати знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп'ютерних систем та середовищ з метою їх запровадження у професійній діяльності.

ПРН 7. Обґрунтовувати вибір технічної структури та розробляти відповідне програмне забезпечення, що входить до складу інформаційних систем та технологій.

ПРН 12. Розробляти та застосовувати моделі представлення знань, стратегії логічного виведення, технологій інженерії знань, технологій і інструментальних засобів побудови інтелектуальних систем і систем штучного інтелекту

Очікувані результати навчання. У результаті вивчення навчальної дисципліни студент повинен

знати: основні поняття, методи та засоби забезпечення безпеки комп'ютерної інформації для вирішення практичних завдань в інформаційних системах, які виникають при зберіганні, обробці та передаванні інформації.

вміти:

- шифрувати інформацію симетричними і асиметричними методами;
- створювати і перевіряти ЕЦП;
- вміти працювати з криптографічними бібліотеками OpenSSL, CryptoAPI.

2. Зміст навчальної дисципліни

Змістовний модуль 1. Основні положення теорії інформаційної безпеки та захисту інформації.

Тема 1. Основні визначення і поняття теорії захисту інформації. Методи захисту інформації. Історія розвитку. Термінологія. Види загроз, їх системна класифікація. Зловмисники та випадкова втрата даних. Поняття атаки на комп'ютерну систему. Література: [3,5, 6,7].

Тема 2. Симетричні криптосистеми. Блочне шифрування. Структура шифру Фейстеля. Сучасні алгоритми шифрування. Стандарт шифрування даних (DES, AES). Режими шифрування.

Література: [1, 2,4,5,7].

Тема 3. Криптографія з відкритим ключем. Алгоритми криптографії з відкритим ключем. Алгоритм RSA. Обмін ключами по схемі Діффі-Хеллмана.
Література: [1, 3,4,5,7]

Тема 4. Методи забезпечення цілісності даних. Одностороння функція хешування. Колізійно-стійкі функції хешування Whirpool та SHA256, SHA-384, SHA-512.
Література: [1, 4,6]

Тема 5. Електронно-цифрові підписи. Схема створення і перевірки ЕЦП. Алгоритми ЕЦП: Ель-Гамаля, RSA. Сліпа підпис Чома.
Література: [3,4, 5, 7]

Змістовий модуль 2. Технології та методи захисту інформації.

Тема 6. Аутентифікація повідомлень. Методи аутентифікації повідомлень. Код аутентичності повідомлення.
Література: [1, 2,3,4,5]

Тема 7. Поняття ідентифікації, автентифікації та різновиди способів автентифікації. Біометричні засоби автентифікації та контролю. Парольні системи. Основні компоненти та загрози безпеки парольних систем. Оцінка стійкості парольної системи.
Література: [3, 4,5,6,7,8].

Тема 8. Інфраструктура відкритих ключів (PKI). Функції PKI.Сертифікат X509. Сертифікат PGP. Система Kerberos.
Література: [1, 3,5,7,8]

Тема 9. Комп'ютерні віруси та їх властивості. Класифікація вірусів. Основні види комп'ютерних вірусів та схеми їх функціонування. Структура комп'ютерних вірусів. Програми виявлення вірусів та заходи по захисту та профілактиці. Антивірусні пакети.
Література: [3, 5,6,7].

Тема 10. Захист інформації за допомогою міжмережних екранів.
Література: [3, 5,7].

Тема 11. Протоколи AAA.
Література: [3, 5,7].

Змістовий модуль 3. Механізми і політики розмежування прав доступу в ОС.

Тема 12. Формальні моделі доступу. Дискреційна модель доступу.
Література: [3,7,8]

Тема 13. Мандатна модель доступу. Роліва модель доступу.
Література: [3,7,8]

Тема 14. Підсистема захисту в ОС Windows. Підсистема захисту в ОС Linux. Порівняння архітектури Windows та Linux
Література: [3,7]

Тема 15. TCSEC ("Оранжева книга") – перший стандарт у галузі оцінки захищеності комп'ютерних систем. Common Criteria ("Загальні критерії") – європейський стандарт у галузі оцінки захищеності комп'ютерних систем. Нормативні документи системи ТЗІ в Україні.

Література: [3,7].

3. Рекомендована література

3.1. Основна література

1. Niels Ferguson Bruce Schneier Practical Cryptography – Wiley Publishing, Inc., 2008. – 397с.
2. Bruce Schneier Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C, – Wiley ,2002. – 662 с.
3. William Stallings Cryptography and network security principles and practice. Seventh edition – published by Pearson Education, 2017– 767с
4. William Stallings Cryptography and Network Security Principles and Practices, Fourth Edition: – Publisher: Prentice Hall, 2005. – 592 с.
5. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

3.2. Допоміжна література

6. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – ДМК Прес, 2012. – 592с.
7. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах / Под ред. В. Ф. Шаньгина. –2-е изд., Перераб. і доп. –М .: Радио и связь, 2001. –376 с.
8. Н.А. Гайдамакин Теоретические основы компьютерной безопасности. Учебное пособие. Екатеринбург 2008 – 212с.

4. Електронні інформаційні ресурси

1. Курс Мережевої академії Cisco Cisco-Cybersecurity Essentials [Електронний ресурс] Режим доступу: www.netacad.com
2. OpenSSL [Електронний ресурс] Режим доступу:https://www.openssl.org/
3. CryptoAPI [Електронний ресурс] Режим доступу:https://docs.microsoft.com
4. Schneier on Security [Електронний ресурс] Режим доступу: https://www.schneier.com/

5. Форма підсумкового контролю успішності навчання

Іспит.

6. Методи діагностики успішності навчання

Поточне опитування, оцінка виконання лабораторних та самостійних завдань, підсумкове опитування.

Примітки:

1. Програма навчальної дисципліни розробляється вищим навчальним закладом. Програма навчальної дисципліни визначає місце і значення навчальної дисципліни, її загальний зміст та вимоги до знань і вмінь.

2. Програма навчальної дисципліни розробляється на основі освітньо-професійної програми.

3. Форма призначена для складання робочої програми навчальної дисципліни.

4. Вищими навчальними закладами можуть вноситися зміни до форми та змістового наповнення «Програми навчальної дисципліни» залежно від специфіки та профілю вищого навчального закладу.

5. Формат бланка – А4 (210×297 мм).