ВИВЧАЄМО ДОСВІД

Галина РАДЧИК

КОМПЛЕКСНЕ МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ «ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ»

Розглядається комплексне методичне забезпечення дисципліни «Основи захисту інформації» для студентів IV курсу (спеціальність 5.091504 «Обслуговування комп'ютерних та інтелектуальних систем і мереж», що складається з програми, яка об'єднує три розділи, конспекту лекцій, електронного посібника, методичних вказівок для виконання лабораторних робіт, завдань для практичних робіт та контрольної роботи, розроблених програмних продуктів для тестування знань роботи криптографічних алгоритмів).

Інформаційні ресурси в сучасних умовах є одним із найважливіших результатів діяльності людського суспільства. Саме тому особлива увага приділяється захисту інформації. Особливого рівня актуальності набирає це завдання в умовах стрімкого розвитку сучасних інформаційних технологій. Такі технології з кожним роком залучають все більшу частину інформаційних ресурсів у процес електронної обробки, що, в свою чергу, спричинює зріст вимог щодо параметрів програмно-апаратних засобів, які використовуються для захисту. З іншого боку, розвиваються нові системи захисту, побудовані на традиційних підходах. Збільшується кількість та різнорідність кінцевих користувачів, що залучаються до обробки інформаційних ресурсів. У процесі обробки інформації використовуються розподілені, неоднорідні комп'ютерні системи та мережі, політика безпеки яких суттєво відрізняється одна від одної.

Використання комп'ютерів і автоматизованих технологій спричиняє появу низки проблем для керівництва організацією. Дбаючи про безпеку інформації, важливо усвідомлювати наявність ризику, зумовленого автоматизацією і наданням щораз більшого доступу до конфіденційних, персональних чи інших даних. Збільшується кількість комп'ютерних злочинів, що врешті-решт може призвести до економічних втрат. Отже, самоочевидно, що інформація — це ресурс, який потрібно захищати.

Циклова комісія комп'ютерних дисциплін технічного коледжу ТДТУ імені Івана Пулюя постійно працює над створенням і впровадженням нових інформаційних технологій у навчальний процес. Важливим щодо цього є комплексне методичне забезпечення навчального процесу, яке дасть змогу студентам у бібліотеці підготуватись до лабораторних робіт, а також опрацювати відповідні розділи теоретичного курсу, винесені на самостійне опрацювання. Питання, сформульовані до розділів курсу з відповідними посиланнями на розділи конспекту, допоможуть студенту підготуватись до здачі тем упродовж семестру.

Авторка розробила комплексне методичне забезпечення дисципліни «Основи захисту інформації», що читається на IV курсі для студентів, які навчаються за спеціальністю 5.091504 «Обслуговування комп'ютерних та інтелектуальних систем і мереж». Цей комплекс включає в себе:

1. Програму курсу з відповідним поділом на розділи;
2. Ілюстрований конспект лекцій;
3. Електронний посібник, створений засобами мови HTML:
4. Завдання для контрольної роботи (30 варіантів);
5. Задачі для практичних робіт;
6. Розроблені програмні продукти для тестування знань студентів з теми «Афінний шифр II-го порядку» та демонстрації шифрування повідомлень на основі симетричних методів.

Програмою дисципліни передбачено вивчення відповідних розділів:

1. Криптографічні методи захисту інформації (включає теми, які розглядають класичні методи шифрування, теорію чисел, шифрування методом гамування, стандарт шифрування

даних DES, симетричні методи IDEA, RC5, Blowfish, ГОСТ 28147-89, криптосистеми з відкрити ключем — алгоритм RSA);

2. Захист інформації в комп'ютерних мережах (включає теми, що стосуються ідентифікації та аутентифікації користувачів комп'ютерних системах, захисту даних за допомогою брандмауерів (системи firewall), захисту віртуальних мереж, спеціалізованих протоколів мережевої взаємодії (PPTP, L2F, L2TP, SSL, SOCKS);

3. Захист інформації в електронних платіжних системах (включає теми, що стосуються принципу функціонування електронних платіжних систем, персональної ідентифікації за допомогою PIN).

У темах першого розділу наведені приклади шифрування. Теми закінчуються вправами. Вправи можуть суттєво відрізнятися за складністю.

Після вивчення основних тем з першого розділу передбачається перевірка знань студентів у вигляді виконання практичних робіт або здачі тестів. Після вивчення кожного розділу знання студентів перевіряються на основі контрольної роботи.

Конспект лекцій відповідає розділам навчальної програми і є достатньо повним джерелом інформації. У конспекті лекцій представлено такі теми.

Розділ 1. Криптографічні методи захисту інформації.

- Проблеми захисту інформації .
- Основні поняття криптології.
- Класичні методи шифрування.
- Метод одноразового блокноту.
- Афінний шифр I-го порядку.
- Захист інформації з використанням генераторів псевдовипадкових чисел.
- Сучасні симетричні системи. Алгоритм DES.
- Алгоритми шифрування даних IDEA , ГОСТ 28147-89, RC5, Blowfish.
- Асиметричні криптосистеми. Система RSA.

Розділ 2. Захист інформації в комп'ютерних мережах.

- Ідентифікація користувачів у комп'ютерних системах.
- Аутентифікація користувачів у комп'ютерних системах .
- Аутентифікації даних та електронний цифровий підпис.
- Алгоритм хешування повідомлень.
- Генерування та розподіл ключів.
- Класифікація систем захисту інформації (стандарти).
- Особливості фізичного та технічного захисту інформації.
- Класифікація шляхів несанкціонованого доступу та життєвий цикл атак.
- Захист даних за допомогою брандмауерів (системи firewall) .
- Захист віртуальних мереж.
- Спеціалізовані протоколи мережевої взаємодії (PPTP, L2F, L2TP, SSL, SOCKS) .

Розділ 3. Захист інформації в електронних платіжних системах.

- Принципи функціонування електронних платіжних систем.
- Електронні пластикові картки.
- Персональна ідентифікація за допомогою PIN.
- Забезпечення безпеки електронних платежів через Internet.

За розділами і відповідними темами конспекту лекцій розроблений засобами мови HTML електронний посібник з дисципліни «Основи захисту інформації». Він складається не тільки із теоретичного матеріалу, що відповідає програмі, а й включає методичні вказівки до виконання лабораторних робіт та робочу програму.

На рисунку 1 зображено вікно електронного підручника.

Рис.1. Електронний посібник «Основи захисту інформації»

Таке забезпечення дає можливість студентам вивчити питання, винесені на самостійне опрацювання, в електронній бібліотеці, а також ознайомитись із порядком виконання лабораторної роботи та вимогами до оформлення звітів.

Конспект лекцій корисний для широкого загалу читачів, починаючи від школярів старших класів і студентів до адміністраторів ком'ютерних систем.

Лабораторні роботи, що увійшли у комплексне методичне забезпечення, стосуються проблем захисту інформації в комп'ютерних системах і мережах на основі програмних засобів, представлені переліком:

- Програмна реалізація алгоритму за методом Цезаря;
- Шифрування тексту на основі методу одноразового блокноту;
- Шифрування тексту на основі афінного методу І-го порядку;
- Побудова генератора псевдовипадкових чисел;
- Блочні криптосистеми типу DES;
- Дослідження процедури шифрування та дешифрування в криптосистемі RSA;
- Робота з криптопакетом KRYPTON;
- Розробка та дослідження засобів ідентифікації користувачів у комп'ютерних системах;
- Дослідження механізмів вибору таємного та відкритого ключів для асиметричног алгоритму.

Для демонстрації роботи симетричного блокового алгоритму розроблена програма SEDA. Алгоритм реалізований на основі афінного шифру II- порядку. Вікно програми представлено на рисунку 2.

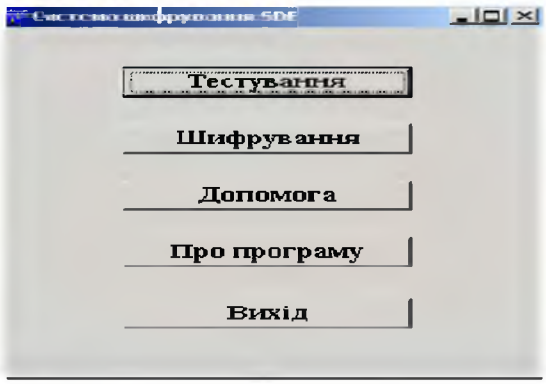

Рис.2. Головне вікно програми SEDA

За допомогою цієї програми можна зашифрувати (розшифрувати) невеликі текстові повідомлення в режимі Шифрування.

Режим Тестування використовується для демонстрації покрокової роботи симетричного алгоритму, як це показано на рисунку 3. Успішне проходження режиму тестування свідчить про те, що студент знає теорію алгоритму.

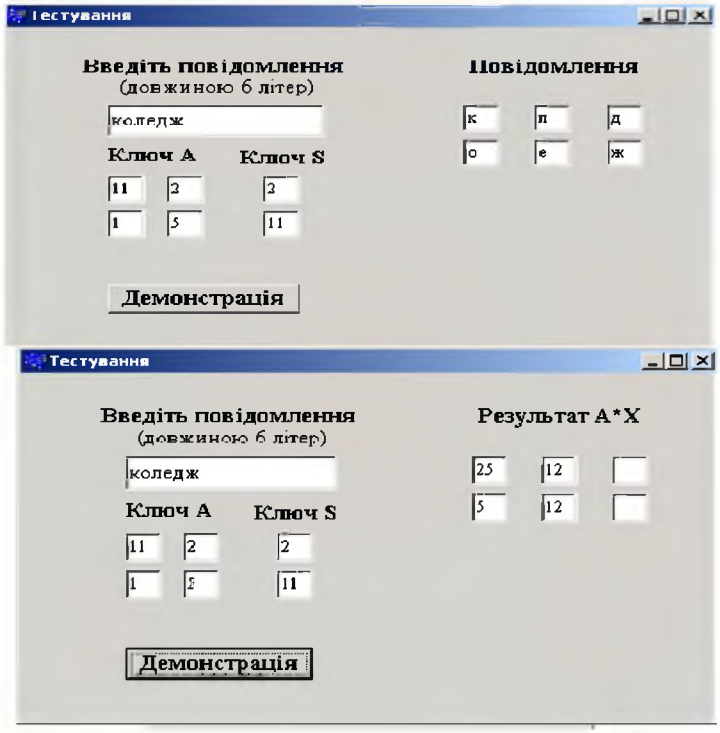

Рис. 3. Покроковий режим шифрування.

Отже, враховуючи важливість проблеми захисту інформації в розвитку інформаційних технологій, це методичне забезпечення може закласти основу сучасного підходу формування компетентності студентів у зазначеній галузі.

ЛІТЕРАТУРА

1. Вербіцький О. В. Вступ до крнптології. — Львів: Вид-во науково-технічної літератури. 1998
2. Гундарь К. Ю., Гундарь А. Ю., Янишевский Д. Я. Защита информации в компьютерных системах. — К.: Корнійчук, 2000.
3. Семків Ю. М. Психолого-педагогічне забезпечення організації ефективної роботи учні комп'ютерних спеціальностей на уроках виробничого навчання // Наукові записки Тернопільського національного педагогічного університету. Серія: Педагогіка. — 2007. — № 7. — С. 137–144.
4. Семків Ю. М. Структурно–логічні основи модульного підходу до організації виробничого навчання та практики учнів комп'ютерних спеціальностей на уроках виробничого навчання. // Наукові записки Тернопільського національного педагогічного університету. Серія: Педагогіка. — 2006. — № 4. — С. 45–49.

Олена САВЧЕНКО

ЕТАПИ АДАПТАЦІЇ ТА ФОРМИ МЕТОДИЧНОЇ РОБОТИ З МОЛОДИМИ ВЧИТЕЛЯМИ

У статті подаються результати досвіду роботи з молодими вчителями з метою їх швидшої адаптації до роботи в школі. Акцентована увага на етапах адаптації (установчий, навчальний, практичний, теоретичного осмислення, підсумково-контрольний), формах і методах методичної роботи з молодими вчителями з різних дисциплін.