Таким чином кожен студент повинен виконати всі три завдання, подати викладачеві для оцінювання проекти *Ceasar_enc.cwm, Ceasar_dec.cwm* та *Ceasar_analisys.cwm*, проаналізувати отримані результати, зробити висновки про взаємодію учасників інформаційного обміну, усвідомити особливості криптографічних методів шифрування та аналізу зашифрованих повідомлень, встановити відношення між поняттями, що вивчаються, на основі використовуваних модульних компонентів середовища CrypTool 2.

Під час підрахунку балів оцінювання підлягають: рівень знань, необхідний для виконання лабораторної роботи, повнота, якість та вчасність її виконання. Також з метою контролю засвоєння знань та вмінь студентами наприкінці лабораторної роботи доцільно провести співбесіду або комп'ютерне тестування для з'ясування рівня засвоєння знань теоретичного матеріалу та основних понять класичної криптології.

Отже, як свідчить практика, впровадження та застосування у процес навчання криптології програмного засобу CrypTool 2 сприятиме підвищенню ефективності навчального процесу, забезпечить можливості розв'язування широкого кола задач з криптології, в тому числі за створеною студентом комп'ютерною моделлю. Очевидно, що дії шифрування та зламу шифру можна виконати вручну, проте це значно збільшить витрати часу на розв'язування задач. До того ж результати ручного шифрування або зламу шифру довгого тексту можуть містити багато неточностей і помилок.

Перспективи дослідження полягають у детальному розгляді можливих шляхів впровадження спеціалізованого програмного забезпечення у процес навчання криптології, розробці та описі методів, прийомів та засобів його застосування при підготовці фахівців з інформатики до захисту інформаційних ресурсів, що сприятиме підвищенню пізнавального інтересу студентів до дисципліни, формуванню їх готовності до подальшої навчальної та професійної діяльності.

Література

1. Жалдак М. І. Проблеми інформатизації навчального процесу в середніх і вищих навчальних закладах/ М. І. Жалдак // Комп'ютер у школі та сім'ї. – 2013. – №3. – С. 8-15.
2. Коляда М. Г. Концептуальні методологічні підходи в професійній підготовці майбутніх фахівців в галузі інформаційної безпеки. [Електронний ресурс] / М. Г. Коляда // Інформаційні технології в освіті. – 2009. – № 3. – Режим доступу: http://ite.kspu.edu/webfm_send/507
3. Горбенко І. Д. Прикладна криптологія. Теорія. Практика. Застосування: монографія / І. Д. Горбенко, Ю. І. Горбенко; Харк. нац. ун-т радіоелектрон., Приват. АТ «Ін-т інформ. Технологій». – Х.: Форт, 2012. – 868 с.
4. Sibylle Hick. Reducing the complexity of understanding cryptology using CrypTool [Електронний ресурс] / Sibylle Hick, Bernhard Esslinger, Arno Wacker. – Режим доступу: http://www.iiis.org/CDs2012/CD2012SCI/EISTA_2012/PapersPdf/EA678TR.pdf
5. Kulwinder Kaur. Performance evaluation of ciphers using CrypTool 2.0 [Електронний ресурс] / Kulwinder Kaur // International journal of computers & technology. – Режим доступу: http://cirworld.org/journals/index.php/ijct/article/view/426/78
6. About CrypTool 2 [Електронний ресурс]. – Режим доступу: http://www.cryptool.org/en/cryptool2
7. Загацька Н. О. Огляд різних версій пакету CrypTool як засобу захисту інформаційних ресурсів. [Електронний ресурс] / Н. О. Загацька // Інформаційні технології і засоби навчання. – 2012. – № 5(31). – Режим доступу: http://journal.iitta.gov.ua/index.php/itlt/article/view/744/548
8. Бабаш А. В. Криптография / А. В. Бабаш, Г. П. Шанкин. – М. : Солон-Пресс, 2002. – 511 с.
9. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький – Л.: ВНТЛ, 1998. – 247 с.
10. Аграновский А. В. Практическая криптографія: алгоритмы и их програмирование / А. В. Аграновский, Р. А. Хади. – М.: СОЛОН-Пресс, 2009. – 256 с.

Твердохліб І.А.
Національний педагогічний університет імені М.П. Драгоманова

Навчання фізико-технічних дисциплін майбутніх вчителів інформатики з використанням комп'ютерного моделювання

Розвиток інформаційно-комунікаційних технологій і масове їх впровадження в навчальний процес школи та ВНЗ стимулюють активний розвиток щодо нового методу пізнання – комп'ютерного моделювання. Його використання в навчальному процесі дає змогу виконувати моделювання реальних технічних пристроїв, не вимагає значних затрат часу та матеріальних ресурсів, а в деяких випадках дає змогу змоделювати роботу технічних пристроїв, розробка чи дослідження яких в реальних навчальних лабораторіях взагалі неможлива.

На думку М.І. Жалдака «використання засобів ІКТ в навчальному процесі має бути педагогічно виваженим і обґрунтоване теоретично та експериментально … доцільне використання сучасних інформаційно-комунікаційних технологій в навчальному процесі дає можливість розкрити значний гуманітарний потенціал природничих дисциплін, пов'язаний з формуванням наукового світогляду, розвитком аналітичного і творчого мислення, суспільної свідомості і свідомого ставлення до навколишнього світу» [2]. Тому, підготовка майбутніх вчителів інформатики повинна сприяти не тільки оволодінню прийомами роботи з програмними засобами загального та спеціального призначення, а й формуванню навичок розв'язування навчальних задач, здійснення дослідницької діяльності, оволодіння методами наукового пізнання з використанням комп'ютерного моделювання.

На думку багатьох дослідників важливим результатом вивчення інформатичних дисциплін є розширення й поглиблення теоретичних основ предметної галузі, що вивчається, за рахунок надання студентам можливості моделювання, імітації досліджуваних процесів і явищ, організації на цій основі дослідницької діяльності майбутніх вчителів, уміння створювати комп'ютерні моделі та проводити експерименти за їх допомогою [9].

Під комп'ютерним моделюванням автори [3] розуміють метод розв'язування задач аналізу або синтезу складної системи, що ґрунтується на використанні її комп'ютерної моделі, тобто сутність комп'ютерного моделювання полягає у відшуканні кількісних і якісних результатів з використанням наявної моделі та її аналізу за допомогою засобів комп'ютерної техніки.

Комп'ютерне моделювання неминуче ставить перед дослідником питання про вибір середовища для моделювання, адекватного досліджуваній проблемі, а у випадку наукових досліджень, що проводяться в певній предметній галузі, сьогодні намагаються працювати у спеціалізованих середовищах, для яких характерним є певний рівень універсальності [4].

Як відомо, для створення сучасних електронних систем і приладів використовують інформаційне моделювання, зокрема математичне. Проте, побудова фізичних моделей багатьох сучасних електронних приладів в навчальній лабораторії вимагає значних затрат часу на підготовку установки, великих матеріальних затрат на обладнання лабораторії, а в деяких випадках, взагалі неможлива. Тому альтернативою до класичного виконання лабораторних робіт є постановка дослідів з використанням віртуальної лабораторії на персональному комп'ютері. Робота у віртуальній лабораторії дає змогу проводити більшу кількість дослідів за той самий час, і при цьому студенти залишаються застраховані від помилок, пов'язаних з виведенням з ладу приладів та радіоелементів, від ураження електричним струмом тощо.

Важливе значення в системі фахової підготовки майбутніх вчителів інформатики відіграє вивчення ними фізико-технічних дисциплін, що сприяє формуванню в них важливих предметних компетентностей, розумінню принципів роботи комп'ютерної техніки, вмінь налагоджувати роботу та усувати певні технічні несправності. До таких дисциплін варто відносити перш за все "Фізику", "Основи мікроелектроніки", "Логічні основи інформатики", "Спеціальний лабораторний практикум з інформатики" тощо.

Неналежний стан, а в деяких випадках і відсутність необхідного лабораторного устаткування, спонукало до пошуку альтернативних шляхів вивчення фізико-технічних дисциплін в процесі підготовки студентів напряму підготовки 0403 – "Системні науки та кібернетика". Так, одним із шляхів інтенсифікації процесу навчання фізико-технічних дисциплін у вищому педагогічному навчальному закладі вбачається у створенні комп'ютерного лабораторного практикуму, який будується на тих самих принципах, що і звичайний лабораторний практикум.

Для організації віртуального лабораторного практикуму будемо використовувати системи автоматизованого проектування (САПР), під якими автори [8, с. 47] розуміють проектування, коли окремі перетворення описів об'єкта, алгоритму його функціонування або алгоритму процесу його створення, здійснюються в автоматизованому режимі.

В державному стандарті України система автоматизованого проектування визначається як автоматизована система, призначена для автоматизації технологічного процесу проектування виробу, кінцевим результатом якого є комплект проектно-конструкторської документації, достатньої для виготовлення та подальшої експлуатації об'єкта проектування [1, с. 12].

Серед усього різноманіття систем автоматизованого проектування їх можна класифікувати за галузевим призначенням:

- MCAD (англ. mechanical computer-aided design) – САПР механічних пристроїв (SolidWorks, Autodesk Inventor, КОМПАС, CATIA);
- ECAD (англ. electronic computer-aided design) – САПР електронних пристроїв, радіоелектронних засобів, інтегральних схем, друкованих плат тощо (MicroCap, OrCAD, NI Multisim, AutoCAD Electrical);

- AEC CAD (англ. architecture, engineering and construction computer-aided design) – САПР в галузі архітектури і будівництва (Autodesk Architectural Desktop, AutoCAD Revit Architecture Suite, Piranesi, ArchiCAD).

В процесі навчання фізико-технічних дисциплін майбутніх вчителів інформатики активно використовуються системи автоматизованого проектування типу ECAD. Так, деякі лабораторні роботи з раніше перерахованих дисциплін пропонується виконувати з використанням систем автоматизованого проектування електронних пристроїв, радіоелектронних засобів, інтегральних схем, друкованих плат тощо. Це зумовлене перш за все відсутністю необхідного лабораторного устаткування та орієнтацією на підготовку майбутніх вчителів, а не інженерів.

Аналіз систем автоматизованого проектування типу ECAD дав змогу виокремити три різних типи програмних засобів комп'ютерного моделювання електронних систем та пристроїв (рис. 1.):

- ✓ комерційні потужні автоматизовані системи, що використовуються на професійному рівні використання яких дає змогу моделювати складні аналогові та цифрові схеми, вони оснащені зручним графічним інтерфейсом та великою кількістю вимірювальних пристроїв;
- ✓ комерційні програмні засоби з безкоштовним поширенням із певними обмеженнями. Розробники таких програмних засобів, як MicroCap, OrCAD, Allegro Cadence, NL5Circuit Simulator, DoCircuit пропонують користуватися демо-версіями своїх потужних САПР, проте з обмеженнями на кількість елементів у схемі, не повною бібліотекою компонентів, обмеженнями на побудову певних графіків тощо;
- ✓ вільнопоширювані САПР, за допомогою яких можна реалізовувати майже таку саму кількість функцій як і за допомогою комерційних, проте вони поширюються за відкритою ліцензією.

Рис. 1. Класифікація систем автоматизованого проектування ECAD

На особливу увагу заслуговують системи автоматизованого проектування, створені для використання безпосередньо в процесі навчання. Так, Logisim – вільнопоширюване програмне забезпечення навчального призначення для розробки та моделювання цифрових логічних схем. Воно призначене для підтримки вивчення дисциплін, починаючи від математичної логіки до архітектури та організації комп'ютерів і використовується студентами коледжів та університетів всього світу [10]. Вагомими перевагами Logisim перед іншими аналогічними програмними засобами є його навчальне призначення, можливість русифікації інтерфейсу та робота під управлінням операційних систем Linux, MacOS X та Windows.

Наведемо порівняльну таблицю характеристик та особливостей використання систем автоматизованого проектування. Системи порівнювалися за характеристиками, що важливі для побудови та моделювання аналогових та цифрових електричних схем, зручністю користувацького інтерфейсу, та доцільністю використання в педагогічних університетах.

Таблиця 1

Порівняльна таблиця систем автоматизованого проектування

Характеристики / Назва програми	Призначення	Операційна система	Моделювання аналогових схем	Моделювання цифрових схем	Відносна складність користування (1 – легко, 5 – складно)
Proteus	Технічне	Windows	+	+	4
NI Multisim	Технічне, Навчальне	Windows	+	+	3
LabView	Технічне	Windows, Linux, MacOS	+	+	4
AutoCAD Electrical	Технічне	Windows	+		3
EDWinXP	Технічне	Windows	+	+	4
Electronics Workbench	Технічне, Навчальне	Windows	+	+	1
MeCAD	Технічне	Windows, MacOS	+	+	4
MicroCAP	Технічне, Навчальне	Windows	+	+	3
OrCAD	Технічне	Windows	+	+	4
Allegro Cadence	Технічне	Windows	+	+	5
NL5 Circuit Simulator	Технічне	Windows	+		5
DoCircuit	Технічне, Навчальне	Он-лайн	+	+	1
Ktechlab	Технічне	Linux	+	+	3
Logisim	Навчальне	Windows, Linux, MacOS		+	2
CircutMaker	Технічне	Windows	+	+	4
LTspice/SwitcherCAD	Технічне	Windows	+	+	4
EasyEDA	Технічне, Навчальне	Он-лайн	+	+	1
Qucs	Технічне	Windows, Linux, MacOS	+	+	4
TINATI	Технічне	Windows, Linux	+	+	4
SimOne	Технічне	Windows	+	+	3
gEDA	Технічне	Windows, Linux	+	+	5
IdealCircuit	Технічне	Windows, Linux	+		5
PartSim	Технічне	Он-лайн	+		4

В процесі навчання майбутніх вчителів інформатики був розроблений комплекс віртуальних лабораторних робіт для підтримки навчання фізико-технічних дисциплін засобами САПР. Наведемо перелік лабораторних робіт, що розроблені для виконання з використанням систем автоматизованого проектування:

1) Навчальна дисципліна “Фізика”:
   - Перевірка закону Ома для постійного струму;
   - Визначення опору провідників за допомогою містка постійного струму (містка Уітстона);
   - Перевірка правил Кірхгофа;
   - Вивчення складання взаємно перпендикулярних коливань. Фігури Ліссажу;
   - Дослідження власних коливань у коливальному контурі;
   - Вивчення вимушених електричних коливань у коливальному контурі.
2) Навчальна дисципліна “Основи мікроелектроніки”:
   - Дослідження вакуумного тріода;

- Вивчення будови та принципу дії напівпровідникового діода;
- Дослідження напівпровідникового стабілітрона;
- Вивчення будови та принципу дії біполярного транзистора;
- Дослідження польового транзистора;
- Вивчення аналогових інтегральних мікросхем;
- Дослідження операційних підсилювачів.

3) Навчальна дисципліна “Логічні основи інформатики”:

- Вивчення логічних елементів;
- Вивчення тригерів;
- Вивчення лічильників;
- Вивчення суматорів та дешифраторів;

Зауважимо, що деякі методичні особливості використання систем автоматизованого проектування в процесі вивчення студентами інформатичних спеціальностей фізико-технічних дисциплін описано в роботах [5, 6, 7].

Відносно новим і досить цікавим типом систем автоматизованого проектування електричних та цифрових схем є он-лайн моделювання. Серед он-лайн програмних пакетів, призначених для моделювання електронних процесів у напівпровідникових схемах, варто виокремити EasyCAD, DoCircuit, PartSim. Дані програмні засоби є вільнопоширюваними та написані на базі утиліти SPICE – симулятора електронних схем з відкритим кодом; до них додано велику бібліотеку елементів, наочні та зручні в користуванні вимірювальні прилади (рис. 2). Доцільність використання систем он-лайн моделювання підтверджується тим, що дані системи проектування розроблялися не лише для інженерів, радіолюбителів, а й для студентів та викладачів.

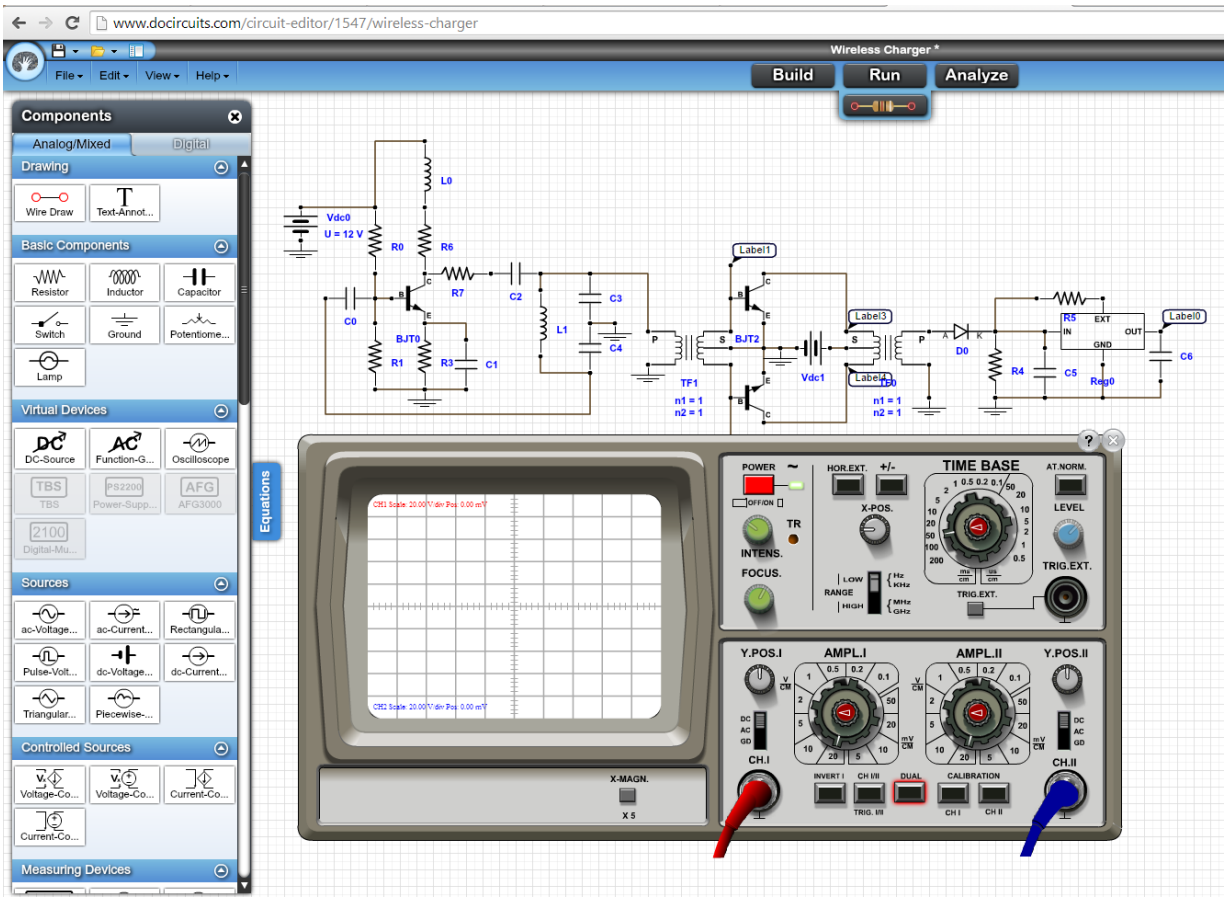

Рис. 2. Робота в САПР DoCircuit в онлайн режимі

Проведення дослідів з використанням віртуальної лабораторії на персональному комп’ютері є альтернативою до класичного виконання лабораторних робіт з фізико-технічних дисциплін за відсутності обладнання для виконання реальних робіт практикуму. Використання комп’ютерного моделювання як методу наукового пізнання в процесі вивчення фізико-технічних дисциплін і поєднання його з методами проблемного навчання сприяє розвитку логічного мислення студентів та формуванню у них системи професійних компетентностей, необхідних у майбутній професійній діяльності.

Отже, вивчення фізико-технічних дисциплін з використанням комп'ютерного моделювання передбачає не тільки формування міцних знань, умінь і навичок з даної предметної галузі, але й сприяє активізації навчально-пізнавальної діяльності студентів, інтенсифікації навчально-виховного процесу та зацікавленості студентів у використанні систем автоматизованого проектування в процесі навчання та в подальшій професійній діяльності.

Література

1. Державний стандарт України 2226-93. Автоматизовані системи. Терміни та визначення. – К.: Держстандарт України, 1994. – 91 с.
2. Жалдак М.І. Система підготовки вчителя до використання інформаційно-комунікаційних технологій в навчальному процесі / М.І. Жалдак // Науковий часопис НПУ імені М.П. Драгоманова. Серія № 2. Комп'ютерно-орієнтовані системи навчання: Зб. наук. праць / Редрада. – К.: НПУ імені М.П. Драгоманова, 2011. – № 11 (18). – С. 3-16.
3. Комп'ютерне моделювання систем та процесів. Методи обчислень. Частина 1: навчальний посібник / [Квєтний Р.Н., Богач І.В., Бойко І.Р. та інші]; за заг. ред. Р.Н. Квєтного. – Вінниця: ВНТУ, 2013. – 191 с.
4. Семеріков С.О. Роль, місце та зміст комп'ютерного моделювання в системі шкільної освіти / С.О. Семеріков, І.О. Теплицький // Науковий часопис НПУ імені М.П. Драгоманова. Серія № 2. Комп'ютерно-орієнтовані системи навчання: Зб. наук. праць / Редрада. – К.: НПУ імені М.П. Драгоманова, 2010. – № 9 (16). – С. 30-40.
5. Твердохлеб И.А. Методические аспекты использования средств ИКТ в процессе обучения компьютерной схемотехнике будущих учителей информатики /И.А. Твердохлеб // Проблемы современной науки: сборник научных трудов: выпуск 10. Часть 1. – Ставрополь: Логос, 2013. – С. 147-154.
6. Твердохліб І.А. Вивчення електродинаміки в віртуальній лабораторії на персональному комп'ютері / І.А. Твердохліб // Матеріали ІІІ міжвузівської науково-практичної конференції "Наукова діяльність як шлях формування професійних компетентностей майбутнього фахівця" (НПК-2012), м. Суми, 5-6 грудня 2012 р. – Суми: Вид-во СумДПУ імені А.С. Макаренка, 2012 р. – С. 276-278.
7. Твердохліб І.А. Віртуальний лабораторний практикум з основ мікроелектроніки / І.А. Твердохліб // Науковий часопис НПУ імені М.П. Драгоманова. Серія № 5. Педагогічні науки: реалії та перспективи. – Випуск 22 : збірник наукових праць / за ред. В.П. Сергієнка. – К.: Вид-во НПУ імені М.П. Драгоманова, 2010. – С. 471-474.
8. Тлумачний словник з інформатики / Г.Г. Півняк, Б.С. Бусигін, М.М. Дівізінюк та ін. – Д., Нац. гірнич. ун-т, 2010. – 600 с.
9. Хазіна С.А. Комп'ютерне моделювання фізичного процесу у різних програмних середовищах / С.А. Хазіна // Науковий часопис НПУ імені М.П. Драгоманова. Серія № 2. Комп'ютерно-орієнтовані системи навчання: Зб. наук. праць / Редрада. – К.: НПУ імені М.П. Драгоманова, 2008. – № 6 (13). – С. 93-96.
10. Logisim web site [Electronic resource]. – Mode of access: http://ozark.hendrix.edu/~burch/logisim/

Біляй І.М.

Національний педагогічний університет імені М.П.Драгоманова

Дослідження залежності графіка функції розподілу ймовірностей від структури подій

Інформаційно-комунікаційні технології стають одним з найважливіших чинників реалізації принципів дидактики в навчанні математики – науковості, наочності, доступності, системності та фундаментальності. Під час вивчення складних понять математики з використанням ІКТ важливу роль можуть відіграти графічні побудови за допомогою засобів інформаційно-комунікаційних технологій, зокрема пакетів математичних програм.

Нині розроблено значну кількість програмних засобів, за допомогою яких можна розв'язувати досить багато математичних задач різних рівнів складності. Це такі програми як GRAN1, GRAN2D, GRAN3D, Advanced Grapher, DG (динамічна геометрія), Wolfram|Alpha, Maxima, MathCad, Maple і ін. Причому одні з цих програм розраховані на фахівців досить високої кваліфікації в галузі математики, інші – на учнів середніх навчальних закладів чи студентів вузів, які лише почали вивчати шкільний курс математики чи основи вищої математики. Для користування програмами GRAN1, GRAN2D, GRAN3D, Advanced Grapher, DG (динамічна геометрія) не обов'язкова наявність надто потужних комп'ютерів з великою швидкодією, значними обсягами оперативної пам'яті чи високими можливостями графічних побудов.