УДК 378:004.056.55

Загацька Н.О.

Житомирський державний університет імені Івана Франка, Житомир, Україна

КОМП'ЮТЕРНА АНІМАЦІЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ НА ОСНОВІ FLASH-ТЕХНОЛОГІЇ ЯК ЗАСІБ ПОДАННЯ НАВЧАЛЬНОГО ЛЕКЦІЙНОГО МАТЕРІАЛУ

DOI: 10.14308/ite000546

Стрімкий розвиток нових інформаційно-комунікаційних технологій (ІКТ) та інформатизація освіти висувають підвищені вимоги до професійної підготовки майбутніх фахівців з інформатики. Серед найважливіших методичних прийомів, що сприяє посиленню мотиваційної складової навчального процесу і, як наслідок, робить його більш ефективним є використання наочності. Перспективним напрямом втілення дидактичного принципу наочності в життя є застосування мультимедійних технологій. За рахунок візуалізації абстрактних об'єктів та явищ, реалізованої комп'ютерними засобами, підвищується рівень доступності складного для сприйняття навчального матеріалу, забезпечується його оптимальне засвоєння та запам'ятовування студентами.

У статті розглядається питання вдосконалення лекційного заняття у вищій школі з фахової дисципліни «Криптологія» за допомогою засобів комп'ютерної анімації на основі flash-технології. Обґрунтовується доцільність застосування мультимедійних додатків як на етапі пояснення нового матеріалу, так і у процесі самостійної роботи студентів. Упровадження комп'ютерної анімації криптографічних алгоритмів на основі flash-технології у освітній процес активізує пізнавальну діяльність студентів та розвиває у них інтерес до навчальної дисципліни. Демонстрацію принципів роботи криптографічних алгоритмів пропонується здійснювати із супроводженням анімованих flash-презентацій на базі середовища CrypTool 1.

Ключові слова: *криптологія, комп'ютерна анімація, flash-технологія, наочність.*

Постановка проблеми. Однією з найпоширеніших форм проведення навчальних занять у ВНЗ є лекція, головне призначення якої забезпечити теоретичну основу навчання, активізувати пізнавальну діяльність та розвинути інтерес до конкретної дисципліни.

Навчальна лекція – це логічно завершений, науково обґрунтований і систематизований виклад певного наукового або науково-методичного питання, ілюстрований, за необхідності, засобами наочності та демонстрацією дослідів. Лекція також визначає напрямок, основний зміст і характер усіх інших видів навчальних занять та самостійної роботи студентів із відповідного навчального предмету [1].

Основною складовою частиною системи підготовки майбутніх фахівців з інформатики є курс «Криптологія», в якому висвітлюються базові поняття, методи та принципи побудови класичних та сучасних алгоритмів шифрування. Варто відзначити, що традиційний підхід до проведення лекцій з цього курсу наразі є малоефективним та має ряд недоліків:

- по-перше, слухачам складно зберігати увагу протягом усього заняття, особливо якщо лекція подається монотонно, відсутнє візуальне супроводження;
- по-друге, студентам досить важко уявити та зрозуміти роботу криптографічних алгоритмів, дані в яких перетворюються в двійковому або шістнадцятковому

вигляді (як правило, шифрування відбувається у декілька раундів, з використанням різноманітних операцій перестановки, заміни, зсуву тощо);
- по-третє, під час традиційної лекції студенти звикають до пасивного сприймання чужих думок, що сповільнює самостійне мислення та звільняє їх від потреби самим здобувати та систематизувати знання.

Отже, виникає необхідність пошуку нових методів, форм та засобів навчання дисципліни «Криптологія» на тих етапах, які є недостатньо ефективними у їх традиційній організації. Вирішити поставлену проблему та вдосконалити лекційне заняття з цієї дисципліни можна завдяки використанню сучасного програмного забезпечення, що дозволяє демонструвати складні криптографічні алгоритми в доступній для засвоєння студентами формі із мінімальними витратами ресурсів. Засоби комп'ютерної анімації на основі flash-технології дають змогу спостерігати за процесом криптографічного перетворення на всіх його етапах, полегшують сприйняття інформації за рахунок її представлення в образному вигляді, таким чином сприяючи реалізації основного принципу дидактики – наочності.

Аналіз останніх досліджень і публікацій. Питання використання ІКТ в освіті висвітлюються в дослідженнях В.Ю. Бикова [2], М.І. Жалдака [3], В.В. Лапінського [4], Н.В. Морзе [5], О.М. Спіріна [6], Ю.В. Триуса [7] та багатьох інших. Шляхи реалізації у навчальній діяльності принципу наочності з використанням сучасних ІКТ розглядали С.А. Волошинов [8], Л.М. Дибкова [9], Т.М. Козак [10] та інші науковці. Створенню та застосуванню інтерактивних flash-технологій при навчанні різних дисциплін присвячені роботи Т.Л. Атаман [11], В.М. Гугніна [12], В.В. Лимаренко [12], Г.А. Швецової [13] та інших.

Аналіз наукових досліджень дають підстави стверджувати, що питання вдосконалення лекційної форми проведення заняття з дисципліни «Криптологія» шляхом використання сучасного програмного забезпечення не було предметом цілісного дослідження і лишається актуальним.

Мета статті – розкрити дидактичний потенціал використання комп'ютерної анімації криптографічних алгоритмів на основі flash-технології у процесі проведення лекційного заняття з дисципліни «Криптологія».

Виклад основного матеріалу. Процес навчання у ВНЗ відбувається у межах різноманітної цілісної системи організаційних форм. Форма організації навчального процесу – спосіб організації, побудови й проведення навчальних занять, у яких реалізуються зміст [14]. Зміст лекційного заняття повинні відповідати наступним вимогам:
- наукова обґрунтованість, інформативність, і сучасний науковий рівень дидактичних матеріалів;
- методично відпрацьована і зручна для сприйняття послідовність викладу та аналізу, чітка структура і логіка розкриття понять;
- глибоке методичне опрацювання проблемних питань лекції, доказовість і аргументованість, наявність достатньої кількості яскравих, переконливих прикладів, фактів, обґрунтувань, документів і наукових доказів;
- яскравість викладу, емоційність, використання ефективних ораторських прийомів виведення головних думок і положень, підкреслення висновків, виклад доступною і зрозумілою мовою, роз'яснення нововведених термінів і назв;
- залучення в пізнавальний процес аудиторії, активізація мислення слухачів, постановка питань для творчої діяльності;
- використання можливостей інформаційно-комунікаційних технологій, засобів мультимедіа, що підсилюють ефективність освітнього процесу.

Зупинимось детальніше на використанні засобів мультимедіа на лекційному занятті. В широкому сенсі «мультимедіа» означає спектр інформаційних технологій, що використовують різноманітні програмні та технічні засоби з метою найбільш ефективного впливу на користувача (що став одночасно і читачем, і слухачем, і глядачем). Завдяки

застосуванню в мультимедійних продуктах і послугах одночасної дії графічної, аудіо (звукової) і візуальної інформації ці засоби володіють великим емоційним зарядом і активно включають увагу користувача (слухача) [15].

Перспективним напрямком використання технологій мультимедіа в навчальному процесі є flash-технологія, що дозволяє створювати та використовувати інтерактивні анімовані мультимедійні додатки із застосуванням векторної графіки. Навчальні flash-ролики відрізняються від традиційної презентації особливою гнучкістю та динамічністю, високою якістю візуалізації досліджуваних об'єктів, займають менший обсяг пам'яті на дисковому просторі та вимагають мінімального часу для завантаження на екран.

Комп'ютерна анімація є потужним інструментом, що дозволяє суттєво підвищити наочність лекційного матеріалу та допомагає утримувати увагу студентів, перетворюючи їх з пасивних спостерігачів в активних учасників навчального процесу. Дослідження показують [10, с. 3], що мультимедійні засоби навчання дають змогу залучати кілька каналів сприйняття, за рахунок чого досягається інтеграція відомостей, які доставляються різними органами чуттів. Відомо, що майже 80% інформації сприймається органами зору, і лише 20% – розумовими зусиллями, пам'яттю. Візуалізація дозволяє значною мірою скоротити словесний опис, впливає на розвиток пам'яті, асоціативного, образного та логічного мислення, сприяє ефективнішому і тривалішому засвоєнню навчального матеріалу.

З метою визначення переваг використання flash-анімації у навчальному процесі ВНЗ було проведено опитування студентів та викладачів Житомирського державного університету імені Івана Франка. В анкетуванні взяли участь студенти 4, 5 та 6 курсів спеціальності «Інформатика*». Загальна кількість респондентів становила 123 особи. Результати опитування показують, що 82% респондентів вважають, що візуальне представлення навчального матеріалу з використанням flash-анімації сприяє кращому розумінню теоретичних основ, 68% – тривалішому запам'ятовуванню інформації, 75 % – зосередженню уваги на предметі навчання, 80% – підвищенню інтересу до дисципліни (рис. 1).

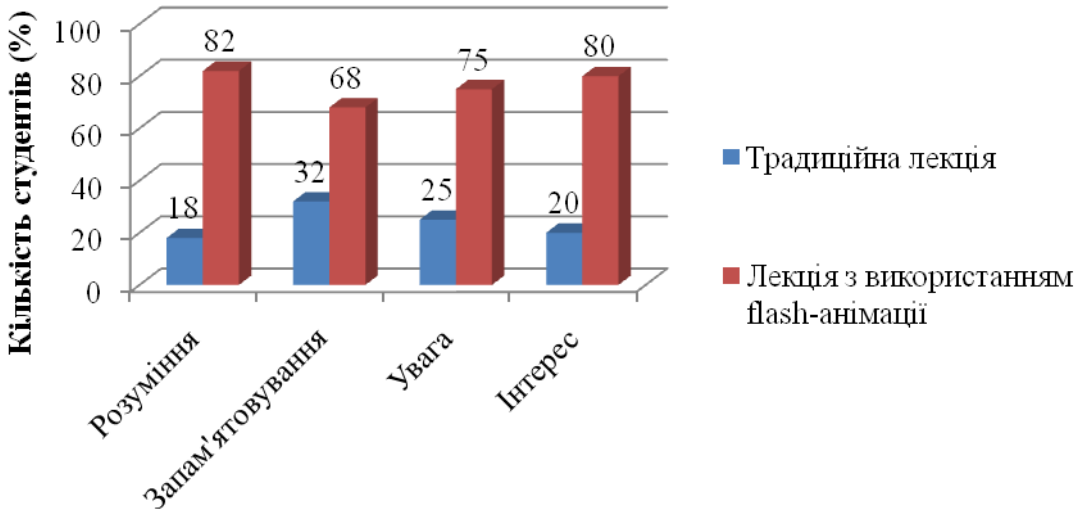

Рис. 1. Результати опитування.

Важливим питанням, що постає сьогодні перед викладачем, є вибір ефективного засобу для подання навчального лекційного матеріалу. Використання наочності має бути педагогічно виправданим, розглядатись передусім з погляду педагогічних переваг, які вона може дати порівняно з традиційною методикою. Основні аспекти, якими потрібно

керуватися при виборі та аналізі навчальних мультимедійних програм та їх застосування, це:

- психологічний – вплив даної програми на мотивацію навчання, на відношення та інтерес до предмета;
- педагогічний – відповідність програми загальній спрямованості курсу та професійній підготовці фахівця;
- методичний – сприяння програми кращому засвоєнню матеріалу, доцільність вибору завдань, методична правильність подання навчального матеріалу;
- організаційний – раціональність планування занять із застосуванням комп'ютера й мультимедійного програмного забезпечення, відведення часу для виконання самостійних робіт.

Сучасні комп'ютерні технології відкривають перед викладачем широкі можливості у виборі та застосуванні засобів навчання із врахуванням специфічних особливостей навчальної дисципліни «Криптологія». Для висвітлення основних понять та нескладних класичних алгоритмів шифрування презентацію лекції можна підготувати із використанням Microsoft Power Point. Проте представити на слайді динаміку складного багатокрокового криптографічного алгоритму, внутрішні взаємозв'язки його складових частин потребує неабияких зусиль та значних витрат часу. Як зазначалося вище, при підготовці лекцій з дисципліни «Криптологія» для досягнення цілей навчання та розуміння предмета особливу увагу варто приділяти питанню візуалізації знань. Тому нами використовується безкоштовне програмне забезпечення CrypTool 1[16], характерною рисою якого є широкий діапазон анімації криптографічних алгоритмів на основі flash-технології. CrypTool 1 створений саме для електронного навчання та задовольняє основним дидактичним вимогам [17].

Досвід впровадження flash-роликів для підтримки навчання дисципліни «Криптологія» на кафедрі прикладної математики та інформатики Житомирського державного університету імені Івана Франка показав їх ефективність у забезпеченні високого рівня подання теоретичного матеріалу. За допомогою засобу CrypTool 1 студентам демонструються найвідоміші алгоритми шифрування – шифр Цезаря, Віженера, DES, AES, протоколи електронного цифрового підпису та обміну криптографічними ключами тощо. До того ж такий спосіб подання навчального матеріалу може використовуватися як доповнення до традиційної лекції, що значною мірою її удосконалює та підсилює, робить більш яскравою і цікавою, інформаційно та емоційно насиченою. Крім того, мультимедійні інструменти CrypTool 1 можна застосовувати на етапі закріплення набутих знань та під час самостійної роботи студентів, що спонукатиме їх до професійного саморозвитку та самовдосконалення, розвиватиме творчий підхід до навчання.

На основі попереднього дослідження було проведено ще одне опитування, яке стосувалося особливостей застосування спеціалізованого програмного забезпечення у процесі навчання дисципліни «Криптологія». Варто зауважити, що 94% опитаних згодні, що покрокова flash-анімація криптографічних алгоритмів допомагає краще сприймати навчальний матеріал порівняно із традиційною лекцією. Крім того, 55% опитуваних зазначили, що користуються спеціалізованим програмним забезпеченням із захисту інформаційних ресурсів під час самостійної підготовки до навчальних занять. З огляду на те, що переважна більшість криптографічних програмних засобів, зорема CrypTool 1, локалізовані англійською мовою, респондентам було поставлено запитання «Чи викликає у Вас труднощі іншомовна (наприклад, англійська) локалізація криптографічного програмного засобу (ресурсу)? », на що 73% респондентів дали відповідь «Ні».

Яскравим прикладом комп'ютерної анімації криптографічних алгоритмів на основі flash-технології є CrypTool-анімація симетричного шифру AES (Advanced Encryption Standard) [18, с. 75], що є найбільш складним для сприйняття студентами. Вивчення цього алгоритму передбачено у рамках теми «Симетричні алгоритми шифрування» згідно робочої програми курсу «Криптологія». На початку лекції, для того щоб викликати інтерес

студентів та підтримувати його протягом усього заняття, потрібно створити чітку мотивацію навчання, продемонструвати зв'язок теми, що розглядається з практикою та з майбутньою професійною діяльністю.

Розгляд роботи алгоритму було б добре почати з питання: «Чому виникла необхідність у появі нового стандарту шифрування?». Таким чином студенти мають пригадати основні характеристики криптографічних алгоритмів, що розглядалися на минулих лекціях і зробити висновок про рівень їхньої криптостійкості. Студентам варто наголосити, що на відміну від вивчених раніше криптосистем, AES базується на архітектурі, для якої характерно представлення блоку у вигляді масиву байтів та виконання криптографічних перетворень, як над окремими байтами масиву, так і над його рядками та стовпцями. Значення байту задається в шістнадцятковій системі числення. Байт розглядають як елемент поля Галуа $GF(2^8)$. Наприклад, многочлен $x^7 + x^5 + 1$ у полі $GF(2^8)$ відповідає 8-бітовому слову 10100001.

Презентація AES складається з двох частин: алгоритму шифрування та процесу утворення ключів. У ній міститься ретельно відібраний та систематизований навчальний матеріал, виокремлено найбільш суттєві поняття та етапи криптографічного алгоритму, відсутні надлишкові математичні обчислення. Спочатку студенти ознайомлюються з узагальненою схемою роботи AES, що відображає процес шифрування у вигляді послідовності раундів (рис. 2). CrypTool-анімація використовує довжину ключа та блока 128 біт. Блок проміжного результату та ключ шифру розглядають як матриці байтів розмірністю 4×4.

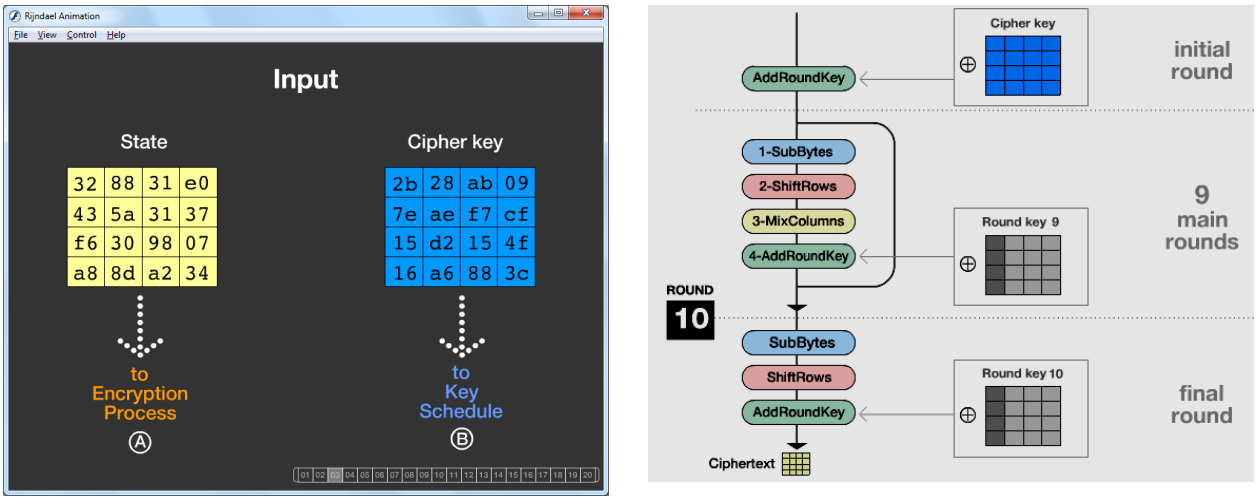

Рис. 2. Flash-анімація алгоритму AES.

Шифрування відбувається у десять раундів. На наступному кроці лекції студентам детально демонструються та пояснюються етапи кожного раунду: 1– підстановка байтів; 2 – зсув рядків; 3 – перемішування стовпців; 4 – додавання раундового ключа (рис. 3). Варто звернути увагу студентів, на той факт, що в останньому раунді пропускається операція перемішування стовпців.

Особливо складним для вивчення в алгоритмі AES є процес утворення ключів. Викладач може спочатку пояснити механізм генерування першого раундового ключа, а потім попросити студентів за аналогією прокоментувати утворення наступних ключів, спонукаючи тим самим аудиторію до спостережливості та самостійної розумової діяльності. Тут варто відзначити провідну роль лектора, як головної дієвої особи лекційного заняття, який повинен не лише вміло користуватися допоміжними наочними засобами, але й здійснювати зворотний зв'язок зі студентами, залучати їх до активного обговорення питань, спільного розв'язання проблем.

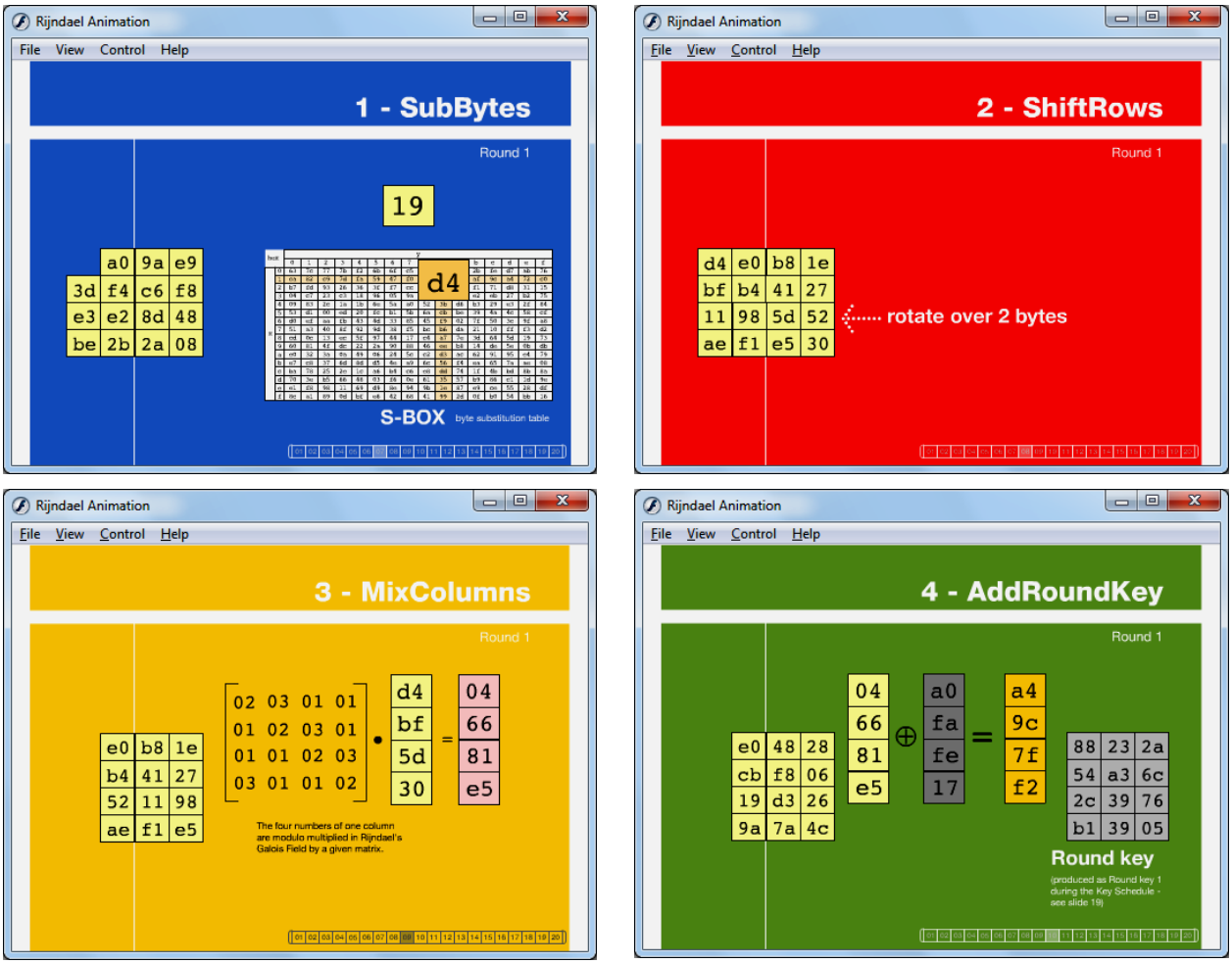

Рис. 3. Flash-анімація 4-ох основних етапів шифру AES.

На ефективність лекції також впливають й інші чинники, такі, як темп подачі матеріалу, його дозування, емоційність викладу, майстерність і стиль спілкування викладача з аудиторією. Поєднання коментарів лектора з flash-анімацією дозволяє досягти максимальної інформаційної наповненості заняття, підтримувати увагу слухачів, виділити найбільш суттєві та важливі моменти. Доцільно підкреслити, що CrypTool-презентація містить достатню кількість ненав'язливих анімаційними ефектів, які призначені для керування черговістю появи об'єктів на екрані. Демонстрація кожного кадру може займати від однієї до п'яти хвилин, що дає змогу студентам повністю засвоїти їх зміст. За необхідності існує можливість повернення до найбільш складних або незрозумілих фрагментів навчального матеріалу.

Flash-презентації лекційного матеріалу із використанням CrypTool 1 мають інтерактивний характер та забезпечують діалог користувача з програмним засобом. Користувач приймає рішення про перегляд відповідного алгоритму і здійснює вибір на екрані потрібного об'єкта за допомогою миші або натисненням на клавіатурі.

Методика читання лекції із використанням комп'ютерної анімації криптографічних алгоритмів на основі flash-технології передбачає наявність роздаткового матеріалу, зокрема схем, таблиць тощо, щоб мінімізувати роботу студентів під час конспектування лекцій і збільшити швидкість подання інформації. Також можна використовувати картки, що містять вільні місця для запису основних положень лекції, які видаються студентам заздалегідь, перед початком заняття (рис. 4). Разом з тим, не вбачаємо обов'язкової потреби у повному конспектуванні студентами усього теоретичного матеріалу, оскільки вони

мають вільний доступ як до текстів лекцій в електронному вигляді, так і до flash-презентацій. Таким чином вивільнений від конспектування час і увагу студент витрачає на осмислення змісту теми. Цей факт особливо важливий в умовах скорочення аудиторних навчальних годин на засвоєння курсу «Криптологія».

AES – це американський стандарт шифрування даних, запропонований на заміну стандарту _____.

AES базується на архітектурі _____. Довжина блока AES ____ біт.

AES дозволяє використовувати три різних ключа довжиною 128, ____ або 256 біт.

Математична база AES:

Для опису алгоритму використовується скінченне поле _____ $GF(2^8)$, побудоване як розширення поля $GF(2) = \{0, 1\}$ по модулю нерозкладного многочлена _____.

Шифрування за алгоритмом AES складається з:

I. Початкового додавання раундового ключа.

II. N_{r-1} раундів, кожен з яких складається з чотирьох етапів:

1. Підстановка байтів;
2. _____ рядків;
3. Перемішування _____;
4. Додавання _____.

III. Завершального раунду N_r, в якому пропускається _____.

Рис. 4. Фрагмент картки для запису основних положень лекції.

Висновки. Узагальнюючи вищенаведене, можна впевнено стверджувати, що використання комп'ютерної анімації криптографічних алгоритмів у процесі проведення лекційного заняття з дисципліни «Криптологія» дозволяє:

- підвищити наочність навчального матеріалу, активізувати пізнавальну діяльності студентів, стимулювати розвиток абстрактного та логічного мислення, посилити мотивацію до вивчення дисципліни;
- системно та найбільш повно розкрити суть і закономірності криптографічних перетворень, чітко виділити структуру лекційного заняття;
- реалізувати доступність інформації шляхом інтегрування візуального та вербального способів сприйняття;
- полегшити розуміння та запам'ятовування теоретичних основ, сприяючи формуванню знань необхідних для засвоєння принципів побудови криптографічних систем;
- привернути увагу аудиторії за рахунок доцільного застосування анімації, демонстрації криптографічних процесів в динаміці;
- забезпечити інтенсифікацію навчання, раціональне та ефективне використання лекційного часу при передачі великого обсягу знань;
- у разі необхідності забезпечити повторення та закріплення пройденого матеріалу.

Лекція – це фундамент, від якості якого залежать результати подальшої навчальної діяльності студента. Досвід застосування комп'ютерної анімації криптографічних алгоритмів на основі flash-технології як засобу подання навчального матеріалу показав його високу ефективність у проведенні лекційного заняття. Гармонійне поєднання основних принципів традиційного навчання та сучасних ІКТ відкриває принципово нові дидактичні можливості для удосконалення форм та методів навчання фахових дисциплін,

дозволяє підвищити рівень підготовки майбутніх фахівців з інформатики, які володіють професійними компетенціями та відповідають сучасним вимогам ринку. Перспективи подальших досліджень убачаємо у вивченні теоретичних і практичних аспектів застосування інтерактивних технологій навчання у процесі проведення лабораторних занять із дисципліни «Криптологія».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Болюбаш Я.Я. Організація навчального процесу у вищих закладах освіти. [Електронний ресурс] – Я.Я Болюбаш // Навч. посібник для слухачів закладів підвищення кваліфікації системи вищої освіти. – К.: ВВП «КОМПАС», 1997.– 64с. Режим доступу: http://www.dut.edu.ua/uploads/l_890_43757791.pdf
2. Биков В.Ю. Основні концептуальні засади інформатизації освіти і головна парадигма прийдешнього суспільства знань / В.Ю. Биков // Я-концепція академіка Неллі Ничкало у вимірі професійного розвитку особистості : зб. наук. пр. / Національна академія педагогічних наук України; Ін-т пед. освіти і освіти дорослих НАПН України. – К., 2014. – С. 32-42.
3. 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.
4. Лапінський В.В. Навчальне середовище нового покоління та його складові // Науковий часопис НПУ імені М.П.Драгоманова Серія №2. Комп'ютерно-орієнтовані системи навчання: Зб. наукових праць / Редрада. – К.: НПУ імені М.П.Драгоманова [Текст], 2008. – № 6 (13) – С.26-32.
5. Морзе Н. В. Моделі ефективного використання інформаційно-комунікаційних та дистанційних технологій навчання у вищому навчальному закладі. [Електронний ресурс] / М. Н. Морзе, О. Г. Глазунова // Інформаційні технології і засоби навчання. – 2008. – № 2 (6). – 8 с. – Режим доступу: http://journal.iitta.gov.ua/index.php/itlt/article/view/138/124#.VB_fhJR_u84
6. Моделювання й інтеграція сервісів хмаро орієнтованого навчального середовища : монографія [Електронний ресурс] / [Литвинова С.Г., Спірін О.М., Шишкіна, М.П. та ін.] ; за заг. ред. С.Г. Литвинової. – К. : ЦП «Компринт», 2015. – 153 с. – Режим доступу : http://lib.iitta.gov.ua/8732
7. Триус Ю. В. Комп'ютерно-орієнтовані методичні системи навчання: монографія / Ю. В. Триус. – Черкаси: Брама-Україна, 2005. – 400 с.
8. Волошинов С.А. Реалізація дидактичного принципу наочності в алгоритмічній підготовці студентів засобами інформаційно-комунікаційного педагогічного середовища [Електронний ресурс] / С.А. Волошинов // Інформаційні технології в освіті/ Херсонський державний університет; гол. ред.: О. В. Співаковський. – Херсон, 2011. – Вип. 10 – 10 с. – Режим доступу: http://ite.kspu.edu/webfm_send/231
9. Дибкова Л. М. Інформаційно-комунікаційні технології як ефективний засіб реалізації у навчальній діяльності принципу наочності [Електронний ресурс] / Л. М. Дибкова // Інформаційні технології і засоби навчання. – 2010. – № 6 (20). – 13 с. – Режим доступу: http://journal.iitta.gov.ua/index.php/itlt/article/view/376#.VYq1XVJcp0I
10. Козак Т. М. Інтенсифікація лекції у вищій школі засобами мультимедійних презентацій [Електронний ресурс] / Т. М. Козак// Інформаційні технології і засоби навчання. – 2012. – № 2 (28). – 11 с. – Режим доступу: http://journal.iitta.gov.ua/index.php/itlt/article/view/651#.VYhGHVJcp0I
11. Атаман Т. Л. Сучасні підходи до навчання інформатики в педагогічному університеті з використанням дистанційних технологій / Т. Л. Атаман // Науковий часопис НПУ імені М. П. Драгоманова. Серія 2 : Комп'ютерно-орієнтовані системи навчання. – 2011. – №. 10. – С. 144-148.
12. Гугнін В. М. Створення засобів тестування для дистанційного навчання на базі технології Flash [Текст] / Гугнін В.М., Лимаренко В.В. // Международная научная конференция MicroCAD : Секція № 14 – Сучасні технології в освіті – НТУ «ХПИ», 2011.
13. Швецова Г. А. Майбутнє – за Flash-технологіями навчання студентів педагогічних ВНЗ / Г. А. Швецова// Гуманітарні науки : Науково-практичний журнал. –2010. – № 2. – С. 49-54.

14. Мешко Г. М. Вступ до педагогічної професії : навч. посіб. / Г. М. Мешко. – К.:Академвидав, 2010. – 200 с. – С. 68-75
15. Риженко С. С. Про досвід використання мультимедійних технологій у навчальному процесі (у ВНЗ) [Електронний ресурс] / С. С. Риженко. // Інформаційні технології і засоби навчання. – 2009. – Том 11, № 3. – 11 с. – Режим доступу : http://journal.iitta.gov.ua/index.php /itlt/article/viewFile/59/45.
16. 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
17. Загацька Н. О. Оцінка якості спеціалізованого програмного забезпечення із захисту інформаційних ресурсів у процесі навчання криптології / Н. О.Загацька // Наукові записки. Кіровоградського державного педагогічного університету імені Володимира Винниченка. Серія: Проблеми методики фізико-математичної і технологічної освіти. Частина 2. – Кіровоград: РВВ КДПУ ім. В. Винниченка, 20154. – Вип. 7. – С. 38-42.
18. Фергюсон Н. Практическая криптография / Нильс Фергюсон, Брюс Шнайер; [пер. с англ. Н.Н. Селиной]. – М.: «Диалектика», 2004. – 432 с.

Natalia Zagatska
Zhytomyr Ivan Franko State University, Zhytomyr, Ukraine

COMPUTER ANIMATION OF CRYPTOGRAPHIC ALGORITHMS BASED ON FLASH-TECHNOLOGY AS TOOL FOR PRESENTATION EDUCATIONAL LECTURE MATERIAL

Rapid development of new information and communication technologies (ICT) and informatization of education places heavy demands on computer science specialists training. Among the most important methodological procedures that conducive to increasing of motivational component of educational process and, as a consequence making it more efficient is the use of visualization. The using of multimedia technology is perspective direction for realization of the didactic visualization principle. By means of visualization of abstract objects and events implemented by computer tools, had been elevated level of perception complicated educational material, ensured its optimal learning and memorizing by students.

The article considers issues improvement the course of Cryptology training at higher school by tools of computer animation based on flash-technology. The practicability using multimedia applications both at the explanation of new material, and in the course of independent work of students is given. The introduction of computer animation of cryptographic algorithms based on flash-technology in the educational process activates the cognitive function of students and develops their interest to the subject. Has been proposed demonstrate cryptographic algorithms with accompaniment of animated flash-presentations based on CrypTool 1.

Keywords: cryptology, computer animation, flash-technology, visualization.

Загацька Н. А.
Житомирский государственный университет имени Ивана Франко, Житомир, Украина

КОМПЬЮТЕРНАЯ АНИМАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ОСНОВЕ FLASH-ТЕХНОЛОГИИ КАК СРЕДСТВО ПРЕДСТАВЛЕНИЯ УЧЕБНОГО ЛЕКЦИОННОГО МАТЕРИАЛА

Стремительное развитие новых информационно-коммуникационных технологий (ИКТ) и информатизация образования предъявляют повышенные требования к профессиональной подготовке будущих специалистов по информатике. Среди важнейших методических приемов, способствующих усилению мотивационной составляющей учебного процесса и, как следствие, делающих его более эффективным является использование наглядности. Перспективным направлением воплощения дидактического принципа наглядности в жизнь является применение мультимедийных технологий. За счет

визуализации абстрактных объектов и явлений, реализованной компьютерными средствами, повышается уровень доступности сложного для восприятия учебного материала, обеспечивается его оптимальное усвоение и запоминание студентами.

В статье рассматривается вопрос совершенствования лекционного занятия в высшей школе по специальной дисциплине «Криптология» с помощью средств компьютерной анимации на основе flash-технологии. Обосновывается целесообразность применения мультимедийных приложений, как на этапе объяснения нового материала, так и в процессе самостоятельной работы студентов. Внедрение компьютерной анимации криптографических алгоритмов на основе flash-технологии в образовательный процесс активизирует познавательную деятельность студентов и развивает у них интерес к учебной дисциплине. Демонстрацию принципов работы криптографических алгоритмов предлагается осуществлять с сопровождением анимированных flash-презентаций на базе среды CrypTool 1.

Ключевые слова: криптология, компьютерная анимация, flash-технология, наглядность.