Міжпредметні курси за вибором у навчальному процесі основної школи

І.А. Акуленко*, Н.О. Красношлик, Ю.Ю. Лещенко

Черкаський національний університет ім. Б. Хмельницького, Черкаси, Україна
*Corresponding author. E-mail: akulenkoira@ukr.net

Paper received 17.07.15; Accepted for publication 25.07.15.

Анотація. Стаття присвячена проблемі розробки й упровадження в навчальний процес основної школи міжпредметних курсів за вибором. Авторами окреслено мету й завдання міжпредметного курсу за вибором для учнів 9-х класів, які вивчають математику поглиблено, «Основи криптології», що забезпечує інтегроване вивчення школярами прикладних аспектів математики та інформатики у контексті теорії захисту інформації. Обґрунтовано його змістове наповнення та окремі методичні підходи й рекомендації щодо вивчення.

***Ключові слова**: курс за вибором, криптологія, шифр, математика, теорія чисел, інформатика*

Вступ. У відповідності до концепції профільного навчання обов'язковим складником сучасного навчально-виховного процесу в школі є курси за вибором. Вони створюють вагоме підґрунтя для забезпечення особистісно орієнтованого навчання й проходження учнем індивідуальною освітньою траєкторією.

Зміст математичних курсів за вибором має розширювати й поглиблювати зміст базової математичної освіти, сприяти позитивній мотивації учнів до опанування нових аспектів математичних знань, до вдосконалення способів математичної діяльності, усвідомлення глибинних зв'язків математики з іншими галузями знань. Тематика курсів за вибором, з одного боку, має враховувати інтереси й уподобання школярів, з іншого, – реалізувати навчальний, виховний, розвивальний, світоглядний, практичний і прикладний аспекти математичних знань, які вони опановують під час допрофільної підготовки (5-9 класи) та під час навчання у профільній школі (10-11 класи). Завдання навчального закладу – забезпечити достатньо широкий спектр тематичної спрямованості математичних курсів за вибором з метою створення сприятливих умов для здійснення учнями основної школи усвідомленого вибору подальшого профілю навчання, розширення їхнього математичного світогляду, ознайомлення з практичними і прикладними аспектами математичних теорій.

Короткий огляд публікацій по темі. Проблематику курсів за вибором у допрофільній підготовці й у профільному навчанні школярів науковці й учителі-практики розробляють у різних напрямах: розглядають їх роль і місце в структурі профільного навчання (В. Кизенко, Л. Орищак, В. Чернега та ін.), розробляють проблематику проектування елективних курсів (В. Беспалько, В. Далінгер, Г. Дорофеєв, А. Каспржак) обґрунтовують загальні положення щодо змістового наповнення програм курсів та їх експертизи (Л. Липова, В. Малишев, П. Замазкіна та ін.), визначають загальні закономірності добору змісту математичних курсів за вибором у допрофільній підготовці та профільному навчанні (М. Бурда, Т. Хмара, О. Шаран, Н. Прокопенко, О. Вашуленко, О. Єргіна та ін.), специфіку математичних курсів за вибором у класах різних профілів (М. Симонова, О. Шаран та ін.), розробляють програми та навчально-методичне забезпечення математичних курсів за вибором у класах різних профілів (Г. Апостолова, О. Морозов, В. Цибко, Г. Лиходєєва, Т. Грицик, О. Єргіна, Д. Требенко, О. Требенко, Л. Канакіна, В. Бевз, Л. Ліпчевський, Ю. Ткач та ін.).

Мета статті – з'ясувати доцільність упровадження в навчальний процес, змістове наповнення та деякі методичні особливості вивчення курсу за вибором «Основи криптології» для учнів 9-х класів із поглибленим вивченням математики.

Матеріали і методи. Як відомо, курси за вибором розподіляють на предметні та міжпредметні [3]. Серед предметних математичних курсів виділяють: 1) курси підвищеного рівня, які узгоджуються з програмовими темами; 2) курси, які поглиблено вивчають окремі розділи програми з математики; 3) курси, в яких вивчаються окремі розділи, що не входять до обов'язкової програми з математики; 4) прикладні, що мають за мету ознайомити учнів зі шляхами та методами застосування математичних знань на практиці, у сучасному виробництві й техніці; 5) курси, присвячені вивченню математичних методів пізнання; 6) курси з історії математики; 7) курси з вивчення методів розв'язування математичних задач. Міжпредметні курси за вибором мають на меті інтеграцію знань учнів з різних галузей знань.

Предметні математичні курси за вибором отримали досить широке представлення, наприклад, у збірнику [3]. Однак сучасний освітній процес вимагає розробки й упровадження міжпредметних курсів за вибором, які поряд із ознайомленням учнів із деякими загальними математичними ідеями, ілюструють застосування математики у різних галузях знань. Однією із таких галузей знань є захист інформації. Тому вважаємо за доцільне упровадити в навчальний процес основної школи курс за вибором «Основи криптології», основною метою якого є цілісне і систематизоване засвоєння учнями змісту окремих математичних понять і фактів, які мають широке застосування в теорії захисту інформації, розширення математичного світогляду учнів, підвищення інтересу до математики та її прикладних аспектів, удосконалення способів математичної діяльності. Досягнення зазначеної мети забезпечується шляхом реалізації таких завдань: 1) формування уявлень учнів про способи захисту інформації; 2) засвоєння учнями теоретичних математичних основ для окремих видів шифрів; 3) формування інтересу учнів до вивчення математичних засад алгоритмів шифрування, поглиблення та розширення їх умінь з програмування; 4) формування уявлень учнів про напрями розвитку сучасної математики та класичних математичних теорій, взаємозв'язків між окремими розділами математики; 5) розвиток творчої активності та індивідуальних здібностей, креативності мислення, інтуїції, пам'яті, уваги.

Теоретичною основою курсу є основи теорії захисту інформації, основи теорії подільності й теорії конгруенцій в кільці цілих чисел (програмовий матеріал 8-го класу з поглибленим вивченням математики), теорії ймовірностей і комбінаторики (програмовий матеріал 9-го класу з поглибленим вивченням математики), основи алгоритмізації та програмування. Зміст курсу органічно пов'язаний зі змістом навчального матеріалу поглибленого курсу математики (8-9 клас) та шкільного курсу інформатики (8-11 клас). Тому він розрахований на учнів 9-х класів із поглибленим вивченням математики або 10-х класів, які вивчають математику на профільному рівні і є інтегрованим міжпредметним курсом. Він розрахований на 17 годин навчального часу й охоплює такі теми: «Класичні шифри» (перше знайомство з шифрами, поліграмні шифри, комбінації шифрів, криптографічний квест), «Афінні шифри» (шифри Цезаря, Віженера, шифр з автоключем, лінійні шифри, афінні шифри, шифр одноразового блокноту), «Асиметричні шифри» (теорема Ейлера, китайська теорема про остачі, алгоритми піднесення до степеня по модулю, асиметричне шифрування, шифр RSA, індекси за простим модулем, протокол обміну ключами Діффі-Геллмана). Орієнтовне календарно-тематичне планування курсу за вибором наведено в [1].

У процесі вивчення курсу за вибором у школярів формуються уявлення про основні класичні способи шифрування й дешифрування за допомогою окремих шифрів та їх комбінацій, як от: шифр частоколу, чотирьох квадратів, Скітала, матричний шифр обходу, шифр Кардано для квадрата й шестикутника, шифр ADFGVX. Передбачено формування уявлень учнів про такі симетричні шифри, як шифри зсуву (Цезаря, Віженера, шифр з автоключем) та афінні монограмні, зокрема лінійні шифри. Окрім уявлень про симетричні криптосистеми передбачено формування уявлень школярів про асиметричні криптосистеми на прикладі шифру RSA, розгляд математичних основ афінних шифрів та шифру RSA, формування вмінь учнів виконувати шифрування й дешифрування повідомлень за допомогою цих шифрів та аналізувати надійність шифрів за допомогою відомого їм математичного апарату.

На першому етапі вивчення курсу для успішного засвоєння процедури шифрування й дешифрування за допомогою шифру частоколу, чотирьох квадратів, Скітала, матричного шифру обходу чи шифру Кардано та ADFGVX учні не відчувають необхідності в додаткових математичних відомостях. На наступному етапі, коли вивчаються афінні шифри, зі школярами необхідно актуалізувати основні поняття теорії подільності та теорії конгруенцій в кільці цілих чисел, з якими вони знайомилися у 8-му класі. Оскільки дешифрування криптотекстів, що отримані за допомогою афінних шифрів, спирається на поняття лінійної конгруенції та її розв'язку, на опановані способи розв'язування лінійних конгруенцій, на алгоритм встановлення наявності й кількості розв'язків лінійних конгруенцій та теорему про лінійне представлення найбільшого спільного дільника двох натуральних чисел, тому на наступному етапі цей навчальний матеріал необхідно додатково розглянути на заняттях курсу за вибором. Вагоме значення мають сформовані вміння учнів застосовувати алгоритм Евкліда для знаходження класу лишків, що є оберненим до даного, застосовувати спосіб перебору, штучний спосіб та спосіб оберненого класу лишків у розв'язуванні лінійних конгруенцій та їх систем. Для подальшого успішного формування уявлень школярів про шифр RSA необхідно повторити поняття простого і складеного натурального числа, властивості простих чисел, китайську теорему про остачі, теорему про канонічне представлення складеного числа. Новими для учнів способами математичної діяльності, на які спирається вчитель під час вивчення асиметричних шифрів, є піднесення до степеня й індексування за простим модулем. У неявному вигляді формується поняття дискретного логарифму.

Для успішного засвоєння учнями змісту нових понять, фактів чи способів діяльності необхідне відповідне навчально-методичне забезпечення. Серед засобів навчально-методичного забезпечення вивчення курсу «Основи криптології» виокремимо навчально-методичний посібник для вчителя [1] та сайт [4], який містить дидактичні матеріали, необхідні для організації й проведення уроків. До кожного уроку даного курсу на сайті описано його мету, вид уроку та представлено електронні матеріали: мультимедійну презентацію, роздатковий матеріал, необхідний для розв'язування учнями вправ, та лістинги програм, що реалізують розглянуті алгоритми шифрування. З їхньою допомогою здійснювалося експериментальне навчання. Зауважимо, що використання відповідного навчально-методичного забезпечення сприяє формуванню методичної компетентності вчителя, а також дозволяє йому інтенсифікувати й урізноманітнити процес навчання.

Результати та їх обговорення. Як показує досвід експериментального навчання, готуючись до перших занять учителю доцільно попередньо ознайомити учнів зі змістом тих основних понять, які є загальноприйнятими в криптології. Зокрема варто зауважити, що криптологія [1, с. 10] – наука про захист інформації, шляхом її перетворення. Ця галузь знань поєднує два напрямки – криптографію й криптоаналіз. Криптографія займається розробкою методів перетворення інформації з метою приховання її змісту, криптоаналіз – дослідженням можливості розшифровування інформації, пошук слабких місць та доведення стійкості шифрів. Основні напрямки використання криптографічних методів – передача конфіденційної інформації, установлення цілісності переданих повідомлень.

Для мотивації навчально-пізнавальної діяльності школярів на початковому етапі навчання вчителю доцільно обирати задачі, що уможливлюють створення проблемних ситуацій, зокрема послуговуючись прикладами з художніх творів [2; 5]. Наприклад, пригадати з учнями відоме оповідання Артура Конан Дойля «Танцюючі чоловічки», за сюжетом якого молодій жінці Ілсі (Elsie) Патрік стали надходити послання із загадковими танцюючими фігурками, і оскільки ні вона сама, ні її чоловік, містер Хілтон Кьюбі, не змогли самі розгадати таємницю, тому вони звернулися до прославленого детектива Шерлока Холмса. Школярі разом із учителем прослідковують за ходом його міркувань і встановлюють зміст зашифрованих повідомлень. У такий спосіб у фоновому режимі формуються основні поняття теорії захисту інформації (алфавіт, відкритий текст, криптотекст, шифр заміни,

шифр перестановки), та уявлення учнів про окремі класичні способи шифрування відкритого тексту й дешифрування криптотексту.

Приклади і вправи для закріплення на заняттях доцільно добирати у такий спосіб, щоб поступово формувати в учнів уявлення про шифри заміни й перестановки. Серед шифрів заміни пропонуємо виокремити монограмні й поліграмні шифри. Прикладами монограмних шифрів є шифр «Танцюючих чоловічків» та інші шифри простої заміни, поліграмних – біграмний (шифр чотирьох квадратів) та триграмний (загальний триграмний шифр) шифри.

Наведемо приклад введення й закріплення триграмного шифру. Нехай маємо дві 3-рядкові таблиці (матриці). Рядки першої складаються з літер алфавіту в «правильному» порядку, у рядках другої таблиці (матриці) літери алфавіту записуються в довільному порядку (рис. 1). Відкрите повідомлення розбиваємо на трійки. Фіксуємо трійки у першій таблиці і «проектуємо» їх на другу таблицю. За таким правилом довільній трійці літер ставимо у відповідність іншу трійку. Отримуємо триграмний шифр. Як показано на рис. 1. слово DOG переходить в AJE.

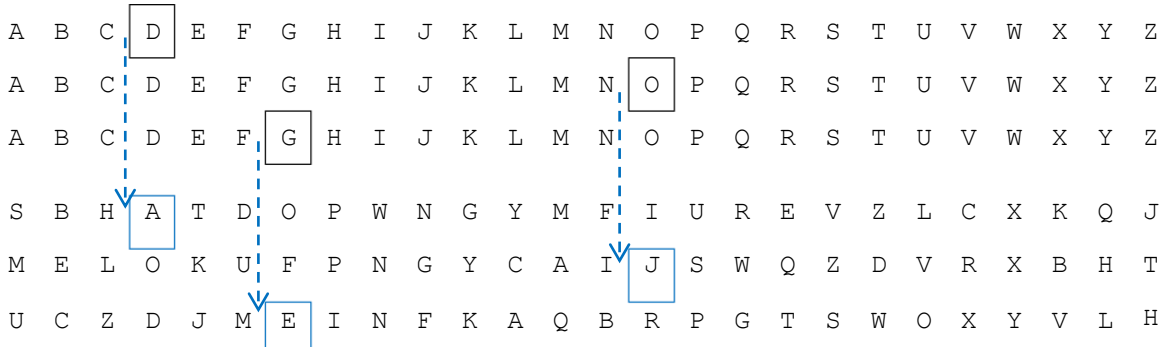

Рис. 1. Триграмний шифр

Роздаємо групам учнів варіанти відкритих текстів і криптотекстів і пропонуємо зашифрувати й дешифрувати повідомлення, використовуючи ключ на рис 1.

Вправа 1. Використовуючи триграмний шифр із заданим ключем (рис.1), зашифруйте повідомлення: 1) intellect; 2) code replacement; 3) decipherment; 4) plaintext.

Вправа 2. Використовуючи триграмний шифр із заданим ключем (рис.2.3), розшифруйте повідомлення: 1) HNTHCJ; 2) VWOSQJ; 3) VSITQJ; 4) FVQBKT; 5) EMDWVS.

Вправа 3. Визначте кількість ключів для наведеного прикладу триграмного шифру.

Із шифрами перестановки доцільно знайомити учнів на прикладах шифру частоколу й матричного шифру обходу. Вагоме додаткове навчальне навантаження цих видів шифрів вбачаємо в тому, що під час дослідження кількості їхніх ключів школярі застосовують знання елементів комбінаторики. Реалізувати при цьому доцільно конкретно-індуктивну схему навчання: від розгляду окремих випадків, а саме, кількості можливих ключів, наприклад, для шифру Кардано розміром 2×2, 4×4, 6×6, 8×8, до узагальнень, а саме, визначення кількості ключів для решітки Кардано розміром $k \times k$. На етапі узагальнення можливо запропонувати учням встановити відповідність між шифрами (шифр простої заміни над n-символьним алфавітом (де ключ – це перестановка символів алфавіту), матричний шифр обходу над n-символьним алфавітом з k-символьним ключем (літери у ключовому слові можуть повторюватися), шифр Кардано з квадратною решіткою $n \times n$, де n – парне число, шифр Кардано з квадратною решіткою $n \times n$, де n – непарне число, шифр частоколу, при умові, що ним шифрується повідомлення довжини n, шифр 4-х квадратів (над алфавітом із 25 символів), шифр ADFGVX з n-символьним ключовим словом (літери у слові не можуть повторюватися, і в алфавіті 36 символів, що більше ніж n)) та формулами, що описують кількість можливих ключів до них ($n!$; n^k; $2^{n^2/2}$; $2^{(n^2-1)/2}$; n; $(25!)^2$; $36!\cdot 26!/(26-n)!$).

У подальшому пропонуємо зосередитися на вивченні симетричних і асиметричних шифрів. Особливості симетричних криптосистем вивчати на прикладі афінних шифрів, асиметричних – на прикладі шифру RSA. Вивчення афінних шифрів доцільно організовувати у такій послідовності: 1) мотивувати введення лінійного шифру; 2) мотивувати вивчення лінійних конгруенцій для успішного дешифрування криптотекстів, що зашифровані лінійним шифром; 3) ввести основні поняття, факти та способи діяльності стосовно розв'язування лінійних конгруенцій; 4) закріпити вміння учнів застосовувати метод спроб і штучний метод у розв'язуванні лінійних конгруенцій, сформувати уявлення про лінійне представлення найбільшого спільного дільника двох натуральних чисел та використання алгоритму Евкліда для знаходження лінійного представлення НСД двох натуральних чисел та знаходження числа, оберненого до даного за визначеним модулем, довести відповідні математичні факти; 5) сформувати вміння учнів застосовувати теоретичні знання щодо властивостей та способів розв'язування лінійних конгруенцій для дешифрування повідомлень, зашифрованих лінійним шифром; 6) мотивувати вивчення афінних шифрів як композиції лінійного шифру та шифру зсуву; 7) розглянути приклади на дешифрування криптотекстів, що зашифровані афінним шифром із невідомим ключем. Способи діяльності вчителя, що реалізують вказану методичну схему детально представлено в [1].

Зауважимо, що ефективність занять курсу за вибором значною мірою залежить від форм організації

навчально-пізнавальної діяльності учнів на заняттях. Важливо, щоб був реалізований діяльнісний і особистісно орієнтований підхід у навчанні. Тому доцільними вважаємо такі нестандартні форми організації занять як урок-криптографічний квест, урок-подорож до криптографічного бюро тощо. Ігрові та інтерактивні форми організації навчання на заняттях курсу за вибором сприяють підвищенню пізнавального інтересу до математики та її міжпредметних зв'язків, удосконаленню способів математичної діяльності. Пропонуємо застосовувати такі інтерактивні вправи як «ажурна пилка», «один-два-чотири», «мікрофон» тощо. Особливу увагу необхідно приділяти етапу рефлексії під час проведення занять курсу, оскільки саме на цьому етапі учні здійснюють рефлексію змісту, процесу та результату своєї навчальної діяльності, а вчитель отримує варіант «зворотного зв'язку», що уможливлює виконання ним контролювальної, коригувальної та прогнозувальної функцій. Ефективними вважаємо вправи на заповнення «екрану рефлексії», структурування або заповнення пропусків у «технологічній карті уроку», вправа «3-2-1» тощо [1, с.15].

Експериментальне навчання засвідчує, що курс за вибором «Основи криптології» має значний потенціал у інтегрованому навчанні математики та інформатики учнів основної школи. На заняттях курсу вчитель інформатики може пропонувати учням фрагменти програм, що реалізують розглянуті на уроці алгоритми шифрування. Розв'язування школярами відповідних вправ (самостійно або з опорою на допомогу вчителя) передбачає розробку ними власних програм. У такий спосіб формується підгрунтя для більш глибокого засвоєння учнями навчального матеріалу й застосування на практиці отриманих знань з програмування. Відповідні навчально-методичні матеріали у вигляді лістингів програм із використанням мов програмування PascalABC.NET (версія 1.8) і Python (2.7) також представлено у навчально-методичному посібнику [1]. Цей матеріал можна використовувати і з метою організації самостійної дослідницької діяльності учнів. Реалізацію алгоритмів шифрування було запропоновано на двох мовах програмування, оскільки нині в загальноосвітніх навчальних закладах ознайомлення учнів з основами алгоритмізації та програмування ґрунтоване, як правило, на вивченні саме мови Pascal. Однак, на нашу думку, Python має певні переваги як «перша мова програмування» через свою простоту та елегантність. Крім того, останнім часом (починаючи з 2014 року) ця мова виходить на чільні позиції серед мов програмування, що вивчаються на початкових курсах у багатьох провідних вищих навчальних закладах світу, що готують спеціалістів з комп'ютерних наук.

Висновки. Результати теоретичного дослідження й експериментального навчання дозволили дійти висновків, що упровадження у навчальний процес основної школи курсу за вибором «Основи криптології» для учнів 9-х класів із поглибленим вивченням математики розширює й поглиблює зміст базової математичної освіти, створює сприятливі умови для позитивної мотивації школярів до опанування прикладних і міжпредметних аспектів математичних знань, до опанування нових способів математичної діяльності.

Роботу виконано за підтримки МОН України (держ. реєстрац. номер 0115U000639).

ЛІТЕРАТУРА

[1] Акуленко І.А. Основи криптології : матеріали курсу за вибором для учнів 9-х класів із поглибленим вивченням математики : навчально-методичний посібник у 2-х частинах. Ч.1 : Симетричні шифри / І.А. Акуленко, Н.О. Красношлик, Ю.Ю. Лещенко. – Черкаси: ЧНУ ім. Б. Хмельницького, 2015 – 112 с.

[2] Верн Ж. Путешествие к центру Земли / Жюль Верн. – М.: АСТ Москва, 2008. – 288 с.

[3] Збірник програм з математики для допрофільної підготовки та профільного навчання / Упоряд. Н.С. Прокопенко, О.П. Вашуленко, О.В. Єргіна. – Х.: Вид-во «Ранок», 2011.

[4] Основи криптології / URL: https://cryptology2015.wordpress.com

[5] По Е.А. Золотий жук / Едгар Алан По. – К. : Дніпро, 2001. – 400 с.

REFERENCES

[1] Akulenko, I.A., Krasnoshlyk, N.O., Leshchenko Yu.Yu. Elements of cryptology : elective course materials for 9th grade with in-depth study of mathematics : textbook for teachers in two parts. Part 1: Symmetric ciphers / I.A. Akulenko, N.O. Krasnoshlyk, Yu.Yu. Leshchenko. – Cherkasy: CNU n.a. B. Khmelnitsky, 2015. – 112 p.

[2] Verne, J. Journey to the center of the Earth / Jules Verne. M.: AST Moskva, 2008. – 288 p.

[3] Collection of pre-profile and profile training programs in mathematics / Comp. N.S. Prokopenko, O.P. Vashulenko, O.V. Ergina. – Kh.: Vyd-vo «Ranok», 2011.

[4] Elements of cryptology / URL: https://cryptology2015.wordpress.com

[5] Poe, E.A. The Gold-Bug / Edgar Allan Poe. – K.: Dnipro, 2001. – 400 p.

Interdisciplinary elective courses in secondary school training

I.A. Akulenko, N.O. Krasnoshlyk, Yu.Yu. Leshchenko

Abstract. The article deals with the problem of elective courses in secondary school training. Authors develop and propose an interdisciplinary elective course "Elements of cryptology". In this paper the principal objective and the structure of the course are presented. The course is designed to combine and develop student's knowledge and skills in Mathematics and Computer Science.

***Keywords**: elective course, cryptology, cipher, mathematics, number theory, computer science*