

11. Хорошко В.О. Методи та засоби захисту інформації : навч. посібн. / В.О. Хорошко, А.О. Четков. – К. : Вид-во "Юніор", 2003. – 502 с.

12. Юзьків Ю.Т. Спільність числових методів афінних перетворень у класичних крипто-системах / Ю.Т. Юзьків, Ю.І. Грицюк // *Захист інформації і безпека інформаційних систем* : матер. І-ої Міжнар. наук.-техн. конф., м. Львів, 31 травня – 01 червня 2012 р. – Львів : Вид-во НУ "Львівська політехніка". – 2012. – С. 134-135.

Грицюк П.Ю., Грицюк Ю.И. Особенности реализации матричной Аф-финной криптосистемы

Рассматриваются особенности разработки надежной криптосистемы защиты информации, которая сочетает матричные Аффинные преобразования, многораундовые действия с различными ключами, а также перестановочный алгоритм, что в целом позволяет значительно повысить ее криптостойкость к грубым атак. Выяснено, что, по сравнению с другими методами защиты, классическая криптография гарантирует защиту информации только при условии, если использовано эффективный криптографический алгоритм, а также соблюдены условия секретности и целостности ключей шифрования. Математически описан алгоритм шифрования/дешифрования информации с помощью многораундовой матричной Аффинной перестановочной криптосистемы с различными ключами шифрования на каждом раунде. Проведенный криптоанализ ее устойчивости показал, что разработанный алгоритм обеспечивают достаточную устойчивость к агрессивным атакам даже за значительный промежуток времени при достаточной производительности вычислительных систем.

Ключевые слова: защита информации, шифрование/дешифрование информации, Аффинная система подстановки Цезаря, криптографическая система Хилла, монограммный и полиграммный шифр, матричные аффинные преобразования, перестановочный алгоритм, криптографический анализ.

Grytsyuk P.Yu., Gryciuk Yu.I. Features of the implementation matrix Affine cryptosystem

The features of the development of robust cryptosystems of information security. The system combines the matrix Affine transformation, multi-round action with different keys, as well as commuting the algorithm. This can significantly increase its crude to the cryptographic attacks. It was found that classical cryptography guarantees the protection of information only on condition, that the cryptographic algorithm used effectively and complied with the conditions of the privacy and integrity of encryption keys. The algorithm encryption/decryption of data using multi-round permutation matrix Affine cryptosystem with a variety of encryption keys for each round is mathematically description. Held cryptanalysis its stability showed that the developed algorithm to provide sufficient resistance to aggressive attacks even for a significant time period at a sufficient performance computing systems.

Keywords: information security, to encryption/decryption of information, Affinity system substitution Caesar, cryptosystem Hill, monogram and poligramy code, cipher matrix Affine transformations, commuting algorithm, cryptographic analysis.

**6. ОСВІТЯНСЬКІ ПРОБЛЕМИ
ВИЩОЇ ШКОЛИ**

УДК 004.42

*Доц. М.С. Пасєка, канд. техн. наук –
Івано-Франківський НТУ нафти і газу*

**ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ
ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ ПЕДАГОГІКИ**

Розглянуто необхідність використання сучасних інформаційних технологій для підвищення професійності підготовки педагогів у вищій школі. Визначено педагогічні етапи й умови формування готовності майбутнього педагога до впровадження сучасних інформаційних технологій у вищому навчальному закладі. Запропоновано структуру професійно-педагогічної інформаційної культури фахівців у галузі педагогіки. Визначено перспективи розвитку у царині застосування інформаційно-комунікаційних технологій у процесі творення віртуально-навчального педагогічного середовища, розробленні методик і технологій формування інформаційної компетенції у фахівців відповідно до галузей знань та дослідження подальшого розвитку ключових життєвих компетентностей особистостей у зв'язку з бурхливим розвитком інформаційного суспільства та глобалізаційними впливами.

Ключові слова: інформаційна компетентність, готовність, інформаційні технології, комп'ютерна грамотність, мислення студентів, готовність.

Актуальність. У сучасному світі підготовка професіональних фахівців – одне з найважливіших завдань вищої школи. Професіоналізм розуміють як високу майстерність, що дає змогу випускнику бути конкурентоспроможним на ринку праці. Підготовка висококваліфікованого фахівця потребує впровадження сучасних інформаційних технологій навчання.

Одним із пріоритетних завдань реформування освіти є підготовка нового покоління педагогів, здатних до професійної діяльності в умовах запровадження сучасних інформаційних технологій у навчальний процес. Інноваційні зміни у педагогіці розпочалися досить давно (40-50-ті роки ХХ ст.) і до наших днів набули широкого розмаху якісного розмаїття, наслідком якого спочатку було створення технічних, аудіовізуальних, електронних засобів навчання, а в останнє десятиріччя – і комп'ютерної підтримки навчального процесу. Появу педагогічних технологій названо четвертою революцією в освіті (після створення шкіл, використання у навчанні письмового слова і винайдення книгодрукування).

Використання комп'ютерної техніки і програмно-інформаційних засобів у навчально-виховний процес у вищій школі дає змогу в комплексі вирішити низку актуальних проблем:

- підвищити інформаційну культуру майбутнього фахівця, зробити доступним для нього світові інформаційні ресурси;
- посилити інформаційну насиченість всього навчально-виховного процесу в закладах освіти.

У процесі поширення інновацій у сфері освіти формується й розвивається сучасна освітня система – глобальна система відкритої, гнучкої, індивідуалізованої неперервної освіти людини протягом усього її життя.

Аналіз попередніх досліджень. Проблеми професійної підготовки фахівців у галузі педагогіки досліджено у багатьох публікаціях вітчизняних і зарубіжних учених: М.Г. Чобітько, С.О. Сисоєва, Т.І. Коваль, А.І. Зязюн, М.О. Шибенюк та ін. Погляди вчених розподіляються на два підходи до стратегії комп'ютеризації освіти. Одні вважають, що головне – це навчання студентів володінню сучасних інформаційних технологій для підвищення професійної підготовки фахівців для їхньої конкурентоспроможності на ринку праці. Інші розглядають освітню стратегію як ланку навчального процесу яка потребує значних змін у методиках, так і змісту освіти. Формування інформаційної культури і впровадження сучасних інформаційних технологій в освіту.

Результати аналізу психолого-педагогічної літератури засвідчили, що у вітчизняній галузі педагогіки достатньо висвітлені концептуальні основи процесу інформатизації системи освіти. У полі зору багатьох учених був педагогічний потенціал інформаційних технологій, досліджували проблему формування інформаційної культури й мислення фахівців у галузі педагогіки, зокрема у працях Л.П. Бабенко, І.Є. Булах, С.Б. Гершунського, Н.В. Морзе, В.М. Монахова, Ю.С. Рамського та інших науковців. Психологічні аспекти використання інформаційних технологій у навчальному процесі досліджено у працях В.М. Бондаревської, Ю.І. Машбиля, В.А. Львовського, В.В. Рубцова та ін. Підготовку фахівця в умовах інформатизації освіти висвітлено в таких працях: Ю.О. Жука, О.В. Майбороди, С.О. Гунька, О.Є. Трофімова, О.І. Шиман й ін.

Ознайомившись з науковими дослідженнями учених, з'ясовано, що, незважаючи на вагомий результати наукових пошуків у цих напрямках, поза увагою залишаються важливі аспекти проблеми формування готовності майбутнього фахівця у галузі педагогіки до впровадження інформаційних технологій навчання у вищій школі. Одним із головних аспектів є організаційно-методичні роботи в цьому напрямі. Труднощі, які виникають у викладачів, пов'язані з недостатніми знаннями категоріальної сутності інформаційних технологій, їхніх класифікаційних параметрів, методичних і практичних засад їхнього ефективного впровадження у навчальний процес вищої школи. Але цих труднощів можна уникнути, якщо готовність майбутнього педагога до використання інформаційних технологій набудатиметься у процесі навчання студентів у вищих навчальних закладах.

Використання сучасних інформаційних технологій у галузі педагогіки

Етапи й умови формування готовності майбутнього педагога. Новітні інформаційні технології відкривають фахівцям у галузі педагогіки доступ до нетрадиційних джерел інформації, підвищують ефективність самостійної роботи, дають нові можливості для творчості, знаходження й закріплення різноманітних професійних навиків, дають змогу реалізувати нові форми й методи навчання.

Прискорений розвиток інноваційних технологій у педагогічних складових навчального процесу приводить до формування нового освітнього середовища. Можна виділити такі основні тенденції: удосконалення змісту навчання; інтенсифікація інтерактивності освітнього середовища; стимулювання активності студента у процесі навчання; організація адаптивного навчального процесу.

Паралельно до цих процесів відбувається впровадження інформаційних підходів до проблеми рівня знань, що дає реалізацію можливостям інформа-

ційним технологіям змінювати освітній процес навчання. Сучасні інформаційні технології відкривають широкі перспективи для візуалізації й інтерактивності навчального процесу. Завдяки новітнім технологіям інформаційного забезпечення стає можливим удосконалення методів освітньої діяльності. Таким чином, з розвитком процесу інформатизації освіти змінюється об'єм і зміст навчального матеріалу, відбувається переструктурування програм навчальних курсів, що приводить до зміни структури й вмісту освіти.

Серед основних проблем інформатизації освіти в навчальному процесі виокремлюють такі:

- формування інформаційної культури фахівця;
- використання нових інформаційних технологій;
- формування навичок щодо організації системної роботи з використанням комп'ютерної техніки в конкретній предметній галузі;
- розроблення сучасних інформаційних технологій;
- підготовка фахівців у галузі педагогіки;
- удосконалення управління освітою;
- ресурсне забезпечення інформатизації освіти.

Підготовку висококваліфікованих фахівців у галузі педагогіки потрібно здійснювати з урахуванням набутого вітчизняного й зарубіжного досвіду, використання новітніх інформаційних технологій. Підґрунтям для цього має бути оновлений зміст, форма організації навчально-виховного процесу відповідно до світових стандартів. Створена модель формування готовності майбутнього педагога передбачає послідовність і наступність у розширенні спектра засобів сучасних інформаційних технологій, якими володіє студент у процесі навчальної діяльності. Розроблена модель водночас передбачає і розширює напрями педагогічної діяльності, в яких фахівець набуває досвіду під час застосування нових інформаційних технологій (рис. 1).

Майбутньому фахівцю недостатньо бути лише компетентним у своїй галузі, а й необхідно добре орієнтуватися в широкому спектрі освітніх технологій, уміти їх використовувати у навчальному процесі, забезпечити якісну підготовку фахівця.

Формування інформаційної культури фахівців у галузі педагогіки.

Формування професійної компетентності майбутніх педагогів перебуває в тісному зв'язку з інформаційною культурою особистості, фахівця й суспільства. Комп'ютерна грамотність зобов'язує використовувати комп'ютерні програмні засоби, працювати з електронним текстом, створювати презентації й бази даних. Тому майбутній педагог має оволодіти ґрунтовними знаннями, сформованими вміннями, навичками, мати певний досвід, бути компетентним у галузі інформатики.

Інформаційна компетентність є новим методологічним підходом у галузі педагогіки, вона дає змогу з'ясувати суть і роль інформаційної компетентності, готовності майбутнього педагога для впровадження інформаційних технологій навчання. Використання можливостей інформаційних технологій для вирішення різних проблем, охоплює різні види діяльності щодо аналізу, подання інформації за допомогою електронних засобів комунікації.

Сформованість інформаційної культури значно полегшує процеси соціалізації майбутнього педагога на різних етапах його професійного становлення, змінюючи не тільки характер його діяльності, а й мислення. Учені Н. Посталок,

М. Габер, Л. Гурова акцентують свою увагу на створенні й впровадженні інформаційних технологій навчання із застосуванням електронних засобів, що формує особливий стиль мислення фахівця. Можна виділити головні характеристики такого мислення: динамічність, гнучкість, творчість, логічність, алгоритмічність тощо. Поняття інформаційної культури й мислення генерується двома фундаментальними поняттями – культура та інформація, відтворення їх взаємозв'язку і взаємовпливу зображено на рис. 2.

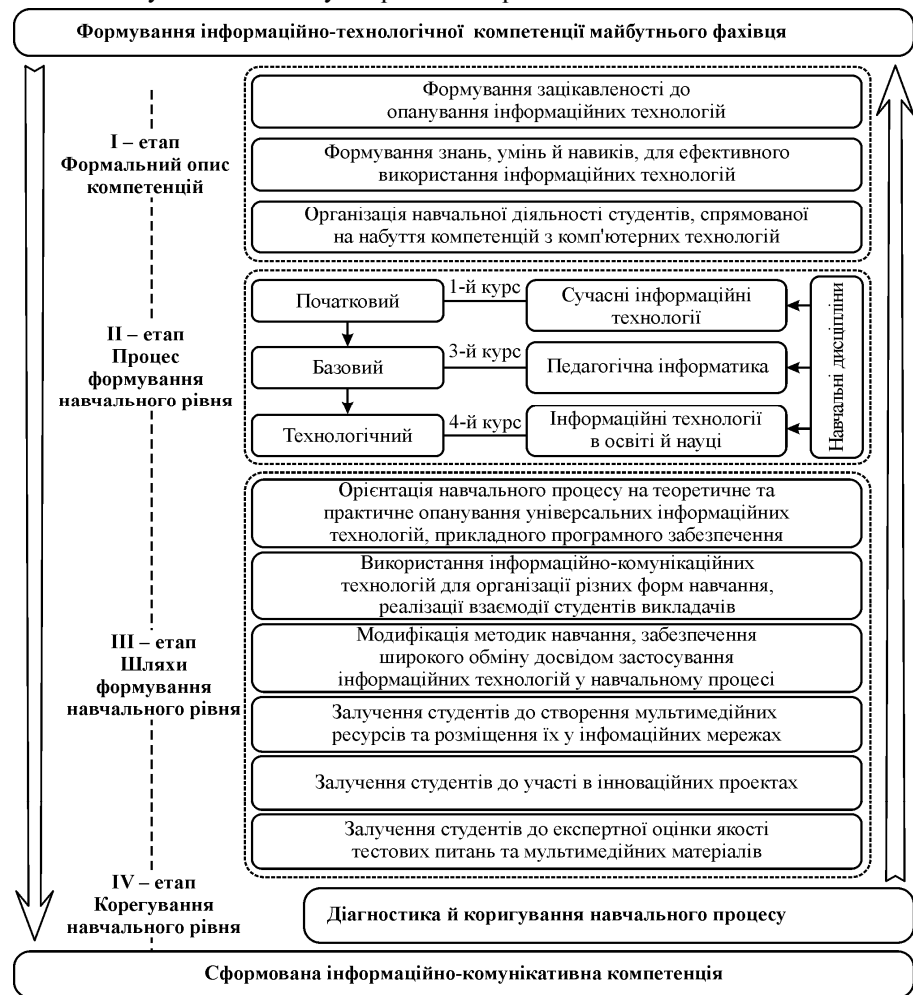


Рис. 1. Модель підготовки висококваліфікованих фахівців

Сьогодні перед фахівцями у галузі педагогіки стоїть важливе завдання – виховати й підготувати висококваліфіковану молодь, спроможну активно включитися в новий етап розвитку сучасного суспільства, пов'язаний зі сучасними інформаційними технологіями навчання.

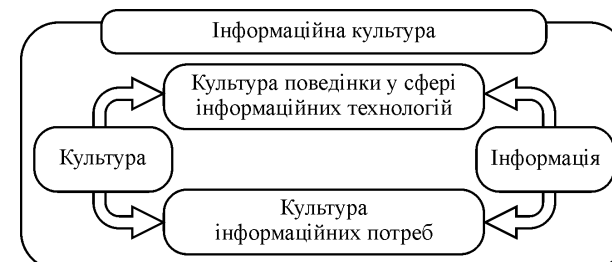


Рис. 2. Генерування поняття інформаційної культури

Успішне входження в професійну діяльність випускник вищого навчального закладу уже має володіти високим рівнем інформаційної культури. До ресурсів інформаційної професійної культури віднесено фаховий і загальнокультурний рівень фахівця в галузі педагогіки. Різні підходи дослідників до визначення поняття інформаційної культури та її місця в професійній культурі педагога зображено на рис. 3. У цій структурі інформаційна культура є "джерелом живлення" всіх інших структурних підрозділів інформаційної професійної культури фахівця.

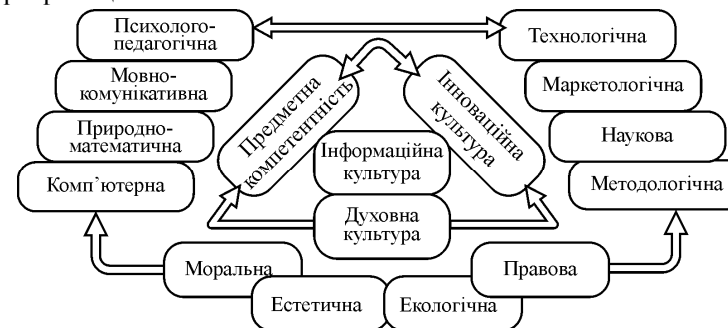


Рис. 3. Структура інформаційної професійної культури

Висновки. За умови використання нових розробок у галузі викладання інформаційних технологій, що базуються на використанні мультимедійних технологій, процес навчання переходить на якісно новий рівень – зараз з упевненістю можна констатувати, що в умовах університету можна змодельовати ситуації реального, природного спілкування. Застосування інформаційних засобів комунікації та інформаційних технологій істотно поліпшує якість подання матеріалу заняття й ефективність засвоєння цього матеріалу, збагачує зміст освітнього процесу та підвищує мотивацію до навчання, надаючи можливість працювати над підвищенням своєї компетенції у зручному для студентів темпі, сприяючи таким чином індивідуалізації навчання та ефективному оволодінню предметною областю. Перспективи розвитку у царині застосування інформаційно-комунікаційних технологій у процесі творення віртуально-навчального педагогічного середовища вбачаємо у детальному дослідженні складників зазначеного вище утворення, розробленні методики та технології формування інформаційної компетенції у фахівців відповідно до галузей знань та дослідження подальшого роз-

витку ключових життєвих компетентностей особистостей у зв'язку з бурхливим розвитком інформаційного суспільства й глобалізаційними впливами.

Література

1. Горячев А.В. Про поняття "інформаційна грамотність" у початковій школі / А.В. Горячев, А.А. Мірошніченко // Відкритий урок. – 2003. – № 9-10. – С. 82-84.
2. Гурін Р.С. Підготовка майбутнього вчителя гуманітарного профілю до застосування нових інформаційних технологій у навчальному процесі загальноосвітньої школи : дис... канд. пед. наук: спец. 13.00.04 / Р.С. Гурін; Південноукраїнський держ. педагогічний ун-т ім. К.Д. Ушинського (м. Одеса). – Одеса., 2004. – 252 с.
3. Горшенин А.Ю. Проблемы построения современного учебника на основе использования ресурсов Интернет / А.Ю. Горшенин // Информационные технологии в обучении и научных исследованиях : матер. 47 науч.-метод. конф. Университетская наука – региону. – Ставрополь : Изд-во СГУ, 2002. – С. 22.
4. Гончарова О.М. Вдосконалення організаційних форм навчання студентів з використанням інформаційно-комунікаційних технологій / О.М. Гончарова // Нові технології навчання : наук.-метод. зб. / кол. авт. – К. : Ін-т інноваційних технологій і змісту освіти МОН України. – 2008. – Вип. 52. – С. 21-24.
5. Дичківська І.М. Інноваційні педагогічні технології : навч. посібн. [для студ. ВНЗ]. – К. : Вид-во "Академвидав", 2004. – 352 с. – (Альма-матер).
6. Лаврентьєва Г.П. Розвиток наочно-образного мислення дошкільників у комп'ютерно орієнтованому середовищі / Г.П. Лаврентьєва // Нові технології навчання: наук.-метод. зб. / кол. авт. – К. : Ін-т інноваційних технологій і змісту освіти МОН України. – 2008. – Вип. 53. – С. 116-122.

Пасека Н.С. Использование информационных технологий для профессиональной подготовки специалистов в области педагогики

Рассмотрена необходимость использования современных информационных технологий для повышения профессионализма подготовки педагогов в высшей школе. Определены педагогические этапы и условия формирования готовности будущего педагога к внедрению современных информационных технологий в высшем учебном заведении. Предложена структура профессионально-педагогической информационной культуры специалистов в области педагогики. Определены перспективы развития области применения информационно-коммуникационных технологий в процессе создания виртуально-учебной педагогической среды, разработке методик и технологий формирования информационной компетенции специалистов в соответствии с отраслью знаний и исследования дальнейшего развития ключевых жизненных компетентностей личности в связи со стремительным развитием информационного общества и глобализационными воздействиями.

Ключевые слова: информационная компетентность, готовность, информационные технологии, компьютерная грамотность, мышление студентов, готовность.

Pasyeka M.S. The Use of Information Technology in Training of Specialists in the Field of Pedagogy

The necessity of using modern information technologies to enhance the professionalism of teacher training in higher education is justified. Pedagogical stages and conditions of formation of future teachers' readiness to the introduction of modern information technologies in higher education are determined. The structure of professional pedagogical culture of information specialists in the field of pedagogy is proposed. We describe the perspective development in the field of application of information and communication technologies in the process of creating a virtual-learning pedagogical environment, the development of techniques and technologies of formation of information competence of professionals in accordance with the fields of knowledge and research further development of the key competencies of the person in connection with the rapid development of the information society and globalization impacts.

Keywords: information competence, readiness, information technology, computer literacy, thinking skills, willingness.

УДК 712.3(477)

*Методист А.О. Пасічник¹;
доц. В.М. Михайлюк², канд. с.-г. наук*

ОПТИМІЗАЦІЯ ОЗЕЛЕНЕННЯ ТЕРИТОРІЇ ПОЗАШКІЛЬНОГО НАВЧАЛЬНОГО ЗАКЛАДУ ЯК УМОВА ЕКСКУРСІЙНОЇ ПРИВАБЛИВОСТІ

Оптимізація зелених насаджень території Львівського обласного центру еколого-натуралістичної творчості учнівської молоді спрямована на підвищення рівня атрактивності позашкільного навчального закладу з еколого-просвітницькою метою шляхом формування навчально-колекційних відділків різних садово-паркових стилів, відділку плодово-ягідного садівництва, навчально-тематичних мікроландшафтів за ботаніко-географічною ознакою у відкритому і закритому ґрунтах.

Ключові слова: оптимізація озеленення, дендрофлора, екскурсійна діяльність, навчально-тематичний мікроландшафт.

Вступ. Серед важливих пріоритетів діяльності позашкільних навчальних закладів є природоохоронний напрям, який передбачає широке залучення учнівської молоді до охорони довкілля, ознайомлення та оволодіння методами екомоніторингу, формування екологічного світогляду школярів, зокрема й через екскурсійну діяльність. Зелені насадження позашкільного навчального закладу, сформовані за принципами ботанічної колекції деревно-чагарникових і трав'яних рослин культурної та природної флори, виконують науково-пізнавальне, навчально-виховне та естетичне значення.

Екскурсійну діяльність на базі позашкільного навчального закладу можна здійснювати у формі навчально-екологічної стежки, схема якої визначає екскурсійний маршрут для ознайомлення з цікавими ботанічними, зоологічними, природоохоронними та іншими об'єктами на території навчального закладу. Навчально-екологічну стежку використовують з освітньою метою для учнів 5-11 класів (закріплення знань за тематикою уроків; проведення гурткових занять, природоохоронної діяльності, екологічних тренінгів) та з освітньо-пізнавальною метою для дітей дошкільного та молодшого шкільного віку (проведення тематичних, загально-оглядових, навчально-виховних та ігрових екскурсій) [1].

Над проблемою аналізу екологічних аспектів оптимізації зелених насаджень у міських ландшафтах працювало чимало дослідників: В.П. Кучерявий (1984, 1994, 1999), С.А. Яблоков (1994), О.О. Лаптев (1998), М.Д. Гродзинський (1993) та ін. Використання ландшафтно-екологічного підходу для внесення планувально-просторових змін та оптимізації озеленення території еколого-натуралістичного позашкільного навчального закладу з метою формування цікавого екскурсійного об'єкта зумовлює актуальність розроблюваної тематики.

Мета дослідження. Виявити залежність екскурсійної привабливості території позашкільного навчального закладу від заходів з реконструкції зелених насаджень, зокрема й функціонального зонування території.

Об'єкти та методика дослідження. Реконструкцію озеленення території проведено з метою вдосконалення еколого-просвітницької діяльності позашкільного навчального закладу на засадах порівняльної екології [2]. Формування насаджень у садово-паркових відділках виконано засобами ландшафтного ди-

¹ Львівський обласний центр еколого-натуралістичної творчості учнівської молоді;

² Надслучанський інститут НУВГП, м. Березне Рівненської області