3. Моторіна В. Г. Дидактичні і методичні засади професійної підготовки майбутніх учителів математики у вищих педагогічних навчальних закладах : дис. ... д-ра пед. наук: спец. 13.00.04 «Теорія та методика професійної освіти» / Валентина Григорівна Моторіна. – Х., 2005. – 512 с.

4. Семенець С. П. Наукові засади розвивального навчання в системі методичної підготовки майбутніх учителів математики : монографія / С. П. Семенець. – Житомир : Вид-во ЖДУ ім. І. Франка, 2010. – 500 с.

5. Скафа Е. И. Средства формирования методической компетентности будущего учителя в системе эвристического обучения математике / Е. Скафа // Mathematics and Informatics / journal of education research. – vol.56. – number 3, Sofia, 2013. – С .211–223.

6. Скворцова С. О. Контекстне навчання як технологія формування професійної компетентності вчителя математики / С. О. Скворцова // Вісник Черкаського університету: Серія: Педагогічні науки. – Черкаси, 2010. – Вип. 191. – Ч.1. – С. 127-131.

Виокремлено та обґрунтовано сучасні проблеми формування та розвитку методичних компетентностей майбутнього вчителя математики в педагогічних університетах. Одним із завдань підвищення ефективності формування методичної компетентності майбутнього вчителя математики вказано створення в педагогічних ВНЗ такого освітньо-розвивального середовища, при взаємодії з яким у студента формується система професійних компетенцій, на основі якої мають розвиватися особистісні педагогічні якості та основи методичних переконань.

Ключові слова: *методична компетентність вчителя математики, готовність та здатність до методичної діяльності, професійні компетенції.*

Выделены и обоснованы современные проблемы формирования и развития методических компетентностей будущего учителя математики в педагогических университетах. Одной из задач повышения эффективности формирования методической компетентности будущего учителя математики указано создание в педагогических вузах такой образовательно-развивающей среды, при взаимодействии с которой у студента формируется система профессиональных компетенций, на основе которой должны развиваться личностные педагогические качества и основы методических убеждений.

Ключевые слова: *методическая компетентность учителя математики, готовность и способность к методической деятельности, профессиональные компетенции.*

Allocated and reasonably modern problems of formation and development of methodical competence of the future mathematics teacher in pedagogical universities. One of the tasks of increase of efficiency of formation of methodical competence of future math teachers is to develop in pedagogical higher education institutions of an educational and developmental environment when working with the student to develop the system of professional competences, which should develop personal pedagogical quality and methodological foundations of belief.

Key words: *methodical competence of the teacher of mathematics, the willingness and ability to methodological activity, professional competence.*

УДК 004.773

Д.Б. Мехед
м.Чернігів, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА. МЕТОДИ БОРОТЬБИ ЗІ СПАМОМ

Постановка проблеми. Всебічна інформатизація суспільства, збільшення обсягів створюваної, одержуваної і накопичуваної інформації ведуть до зростання актуальності питань, пов'язаних з поширенням спаму, його впливу на інформаційне середовище (простір) організацій [4] і фізичних осіб, ефективність їх діяльності; рівень інформаційної безпеки [2]. Ці питання в літературі розглянуті недостатньо повно.

Метою цієї статті є комплексне дослідження спаму з позицій інформаційної безпеки споживачів інформації (СІ) у взаємозв'язку з компетентністю фізичних осіб та організацій у сфері інформаційно-комунікаційних технологій (ІКТ-компетентності).

Аналіз основних досліджень і публікацій. Дослідженню інформаційної безпеки присвячені роботи В. Баранника, В. Богуна, С. Віхорева, І. Горбенко, Ю. Грицюк, С. Казмирчук, Г. Конаховича, О. Корченка, М. Луцького, А. Марущака, В. Мельнікова, В. Мохора,

О. Новікова, О. Олійника, О. Сосніна, С. Толюпи, В. Хорошко, О. Юдіна та ін.

Становлення і розвиток мережевої теорії та дослідження спаму є предметом зацікавленості Дж. Барнза, Р. Берта, П. Бурдьйо, Дж. Гелбрейта, І. Денисенко, Р. Зиммеля, Р. Інгельгарта, М. Кастельса, О. Князєвої, Дж. Коулмена, А. Мальцевої, К. Мітчелл, Я. Морено, Р. Равід, Р. Радкліфф-Браун, Дж. Рітцера, Н. Романовського, В. Сороки, Б. Уеллмана.

Виділення не вирішених раніше частин загальної проблеми. Проте, незважаючи на значний обсяг накопичених у цій сфері знань, недостатньо дослідженою залишилась проблема організації інформаційної безпеки та боротьби зі спамом.

Поняття спаму, його місце у формуванні інформаційного середовища фізичних осіб та організацій.

Більшість користувачів Інтернету в Україні стикається зі спамом російською та українською мовами (іноді у вигляді низькоякісного «автоматичного» перекладу з іноземної), рідко – англійською мовою. За [6] спам – це розсилка комерційної та іншої реклами або інших видів повідомлень (інформації) особам, які не висловлюють бажання їх отримувати. В українській мові термін спам зазвичай застосовується щодо розсилки листів електронною поштою (ЕП). Одним з напрямків досліджень у галузі захисту інформації є розробка методів і алгоритмів фільтрації потоку електронної пошти. Останнім часом електронна пошта стала одним з найбільш поширених засобів зв'язку, управління та бізнесу. Вона є досить досконалою в технічному відношенні і недорогою альтернативою звичним засобам зв'язку.

Разом з розвитком електронної пошти збільшується і кількість загроз її нормальному функціонуванню. Загальне зростання обсягів інформації, одержуваної фізичними особами та організаціями, супроводжується зростанням частки спаму. Це призводить до відволікання ресурсів СІ на аналіз непотрібної інформації і її видалення з пошти, затримує ухвалення необхідних рішень та ін. Спам – це в основному настирлива реклама різних товарів і послуг, включаючи ті, які не можуть рекламуватися легальним чином [6] – наприклад, контрафактної продукції, незаконно отриманих баз даних тощо. В спамі, що розповсюджується у формі листів по ЕП, також зустрічаються: відомості, які прямо паплюжать конкурентів, що заборонено чинним законодавством України про рекламу; інформація, яка розсилається від імені конкурентів; спроби шахрайства у тому числі шляхом зазначення номерів телефонів, на рахунки яких необхідно переказати гроші; фішинг (захист від нього почали вбудовувати в Інтернет-браузери); пропагандистські матеріали, включаючи передвиборчу рекламу та ін.

Ми розглядатимемо спам, представлений у звуковій формі, на паперових носіях та в електронній формі. Останній вид спаму зараз переважає, тому питання формування та підвищення ІКТ-компетентності СІ, користувачів персональних електронних обчислювальних машин (ПЕОМ) має важливе значення. Згідно з [6] оцінкою, збитки від спаму для економіки тільки України за 2014 рік (з посиланнями на різні джерела) складають від 5 до 27 млрд. грн / рік. У той же час джерела спаму Українського походження (у тому числі ті, що використовують для розсилки сервери і поза Україною) завдають значної шкоди СІ в інших країнах. За підсумками дослідження Лабораторії Касперського Україна входить в десятку лідерів з поширення спаму [7].

Найважливіший канал поширення електронного спаму – листи, що приходять по ЕП (вони можуть містити шкідливий код – їх відкриття може спричинити до самопоширення спаму). На початковому етапі впровадження Інтернету в Україні багато фізичних осіб та організацій користувалися компонентом Outlook Express операційної системи Windows в комбінації з скриньками ЕП, наданими місцевими провайдерами послуг доступу до Інтернету. При цьому зазвичай доводилося приймати всю вхідну пошту (у порядку її потрапляння до скриньки), включаючи спам. Пізніше почали використовуватися поштові програми типу «Thebat!» – вони давали можливість переглянути список повідомлень, що прийшли (і їх розміри), відразу видаляти непотрібні без здійснення прийому. Потім досить швидко відбувся перехід більшості користувачів на використання безкоштовних (для користувачів) порталів електронної пошти всеукраїнського або міжнародного характеру з широкими функціональними можливостями.

Наразі існують технології створення фільтрів-сервісів відсікання нав'язуваної інформації. Їх прийнято розділяти на два класи ті, що налаштовуються вручну і автоматизовані. Технології першого класу застосовують списки доступу і налаштовуються користувачем, який обирає або заборону, при політиці «чорного списку», або дозвіл, при політиці «білого списку», отримання листів з певної адреси. Але такий поділ вхідної інформації неефективний, оскільки передбачає часте оновлення списків доступу.

Застосування автоматизованих технологій фільтрації засноване на використанні методів розпізнавання образів, штучного інтелекту, застосуванні математичної статистики і т.д. Фільтрам, створеним із застосуванням теорії штучного інтелекту, навчання необхідно лише на самому початку. Вони, в процесі експлуатації, продовжують навчатися самостійно. При цьому помітно знижується навантаження на користувача. Зараз такі компоненти є в багатьох «антивірусних комплектах». Портали ЕП активно конкурують між собою за користувачів, що позитивно впливає на ефективність боротьби зі спамом. Типова автоматична фільтрація спаму на основі вихідних адрес повідомлень (у тому числі шляхом перевірки їх наявності в «чорних списках»); кількості зазначених у листі адресатів; заголовків і змісту повідомлень. Зазвичай рішення про віднесення до спаму має багатокритеріальний і нечіткий за своїм характером [5]. При цьому можуть виникати два види помилок: неправильна діагностика як спаму «звичайного» листа та «пропуск» спаму в поштову скриньку СІ. Користувачам не повідомляється про «відсічені» повідомлення, що іноді може завдавати їм серйозну «інформаційну шкоду». Для вибору оптимальних алгоритмів фільтрації спаму слід використовувати математичні моделі оцінки збитків, пов'язаних з неправильною діагностикою. Побудуємо приклад однієї з них. Приймемо, що протягом місяця кількість направлених на адресу ЕП повідомлень становить N за їх кількістю, причому в них частка (ймовірність) спаму становить P(S). Отже ймовірність для «не спам» - листів – $P(\bar{S})=1 - P(S)$. Приймемо, що *P(Q)* – ймовірність правильної діагностики спам-листів як «спаму». Тоді $P(\bar{Q}) = 1 - P(Q)$ вірогідність «пропуску» спам-листа при діагностиці, тобто його діагностики як «не спам». Збиток від одиничного «пропуску» спам-листа приймемо рівним t(Q).

Приймемо також, що ймовірність діагностувати одне «не спам» – повідомлення як спам – P(L), а збиток від такої помилки *t(L)*. Ймовірний збиток, пов'язаний з помилковою діагностикою електронних листів U у рамках бінарної класифікації («спам-не спам»), що враховує обидва типи помилок класифікації, можна обчислити за формулою:

$$U=N\cdot(P(S)\cdot(1-P(S))\cdot t(Q)+(1-P(S))\cdot P(L)\cdot t(L)) \quad (1)$$

Крім «бінарної» можлива класифікація повідомлень на три групи: «спам»; «підозрілі на спам»; «не спам». Таке рішення застосовується, наприклад, на порталі ЕП www.ukr.net- для «підозрілих» повідомлень використовується окрема папка ЕП, звана «спам». Об'єкти з неї автоматично (без попереджень) видаляються після закінчення місяця. Приймемо, що середня імовірність переміщення одного «не спам» – повідомлення в папку «підозрілі» дорівнює P(X), а збиток від такої помилки класифікації дорівнює t(X). Причина збитку – папка з «підозрілими» повідомленнями проглядається рідко, тому лист може застаріти або бути автоматично видаленим з папки. Збиток від переміщення в папку «підозрілі» листи, який фактично є «спамом», незначний і ми його не будемо враховувати. Тоді замість (1) маємо:

$$U=N\cdot(P(S)\cdot(1-P(S))\cdot t(Q)+(1-P(S))\cdot(P(L)\cdot t(L)+P(X)t(X)) \quad (2)$$

Ще одна опція, яка використовується на порталах ЕП – можливість користувачів поскаржитися на спам, у тому числі простим натисненням кнопки. Абсолютна більшість таких порталів не пропонують СІ можливостей індивідуальної налаштування антиспамових фільтрів та автоматичного розподілу вхідних електронних повідомлень по створених ними папках. У ряді великих організацій та їх груп (наприклад, сукупностей академічних інститутів) є «внутрішні» системи ЕП. При цьому їх системні адміністратори іноді вносять в «чорні списки» навіть загальнопоширені портали ЕП. Через це не доходять важливі повідомлення адресатам, причому без повідомлення відправників про це. Власні системи ЕП зазвичай є і у великих освітніх організаціях – особливо ВНЗ. Викладачі, як правило, отримують власні адреси ЕП, які

використовуються для роботи зі студентами, у тому числі дистанційного навчання. За спам-фільтрацію листів по ЕП, що надходять ззовні ВНЗ, відповідають фахівці його інтернет-служб. Фільтрація може виконуватися з використанням: «штатних» коштів проксі-серверів; додаткових програм, у тому числі власної розробки. У великих організаціях можливий також спам, розповсюджуваний в їх локальних мережах. Його «антиспамова фільтрація» часто не здійснюється, а кількість одержувачів листів не обмежується. При цьому існує можливість «витоку» великих списків адрес назовні ВНЗ [1]. Авторами «внутрішніх» спам-розсилок можуть бути, зокрема, студенти ВНЗ. Такі технології можуть використовуватися: для організації DDOS-атак на сервери різних організацій; розсилки комерційних повідомлень невеликими порціями з різних адрес в різні моменти часу. На окремих ПЕОМ засоби типу файерволів використовуються не завжди. Навіть якщо вони інстальовані і «включені», користувачі які не є ІТ-спеціалістами, часто не можуть в оперативному режимі прийняти правильне рішення про «заборону» або «дозвіл» дій, запитуваних різними програмами, в т.ч. для їх «оновлення».

Для організації розсилок ЕП ключове значення має отримання спамерами адрес користувачів. Можливі наступні варіанти: «злом» баз даних на порталах ЕП в Інтернеті, в соціальних мережах, на серверах організацій; комерційних підгруп чи інші засоби тиску на осіб, які мають доступ до таких баз; покупка таких баз на «чорному ринку»; обмін базами адрес ЕП між спамерами; поширення вірусних програм, що зчитують адреси ЕП з поштових скриньок користувачів, їх адресних книг та ін.; автоматичний збір даних за адресами ЕП з матеріалів на сайтах в Інтернеті; автоматична генерація потенційно можливих адрес ЕП і їх тестування шляхом пробних розсилок (відсутність повідомлення про відмову в доставці може розглядатися як ознака існування адреси ЕП); ручний збір даних з різних паперових та інтернет-джерел. Особливо відзначимо такі джерела отримання адрес ЕП: інтернет-сайти організацій та / або особисті сторінки на них фізичних осіб; особисті сторінки на сайтах соціальних мереж; офіційні документи на паперових носіях; рекламні матеріали організацій – на папері, в Інтернеті; наукові статті в електронній формі та на папері (у більшості видань вказівка адрес ЕП користувачів зараз є обов'язковою) – у тому числі в журналах в електронній формі на сайтах ВНЗ; візитні картки фізичних осіб; результати реєстрації на сайтах в Інтернеті (провідних виробників комп'ютерної техніки та програмного забезпечення це не стосується).

Вплив ІКТ-компетентності фізичних осіб і організацій на ефективність боротьби зі спамом. Юридичні заходи боротьби зі спамом на рівні держав – це в основному прийняття адекватних нормативних актів і їх послідовне виконання. Останнє унеможливлюється тим, що джерела російськомовних спам розсилок часто розташовані поза Україною. Крім того, розсилка спаму може здійснюватися і з тимчасових адрес ЕП, зареєстрованих на вигаданих осіб чи організацій. Організаційні заходи боротьби зі спамом: різні заборони і обмеження для організацій, підрозділів, фізичних осіб – у тому числі у формі регламентів і посадових інструкцій; автоматичний контроль обсягів вхідного і вихідного трафіку користувачів Інтернету та ін.

Відсікання здебільшого спаму зараз здійснюється на порталах ЕП (www.mail.ru, www.google.com.ua, www.ukr.net та ін.), послуги яких постійно удосконалюються. Однак якусь частину спаму їх фільтри пропускають (зазвичай не більше 1-2 % – з урахуванням листів, що потрапляють в «сумнівні»). Відсікання спаму можливо і фільтрами на проксі-серверах організацій – однак це вимагає досить високої ІТ-кваліфікації профільних фахівців.

У рамках шкільної і вишівської освіти користувачі ПЕОМ отримують деякі відомості щодо заходів захисту від спаму. Проте в основному відповідна кваліфікація набувається за рахунок практичного досвіду роботи в Інтернеті. Особливо важлива роль ВНЗ при підготовці фахівців з інформаційної безпеки [2]. Однак у більшості організацій сертифікація знань з комп'ютерної безпеки (як умова допуску до роботи на ПЕОМ та / або в Інтернеті) зазвичай не здійснюється – не тільки щодо користувачів, а й серед ІКТ-фахівців. Базове правило для листів ЕП – не відкривати те, що прийшло з незнайомих джерел, і може призводити до втрат важливої інформації. Для зручності селекції листування, а також забезпечення особистої інформаційної безпеки багато користувачів зараз мають по декілька поштових скриньок на різних порталах ЕП.

При цьому можуть використовуватися засоби збору пошти, які в принципі знижують рівень інформаційної безпеки щодо адрес ЕП [1].

Окрім листів ЕП при роботі в Інтернеті можливі й інші види спаму: «миттєві повідомлення» у вигляді спливаючих вікон; відкриття вікон з рекламними повідомленнями, сторінок незапрошених сайтів і т.п.; розміщення (зазвичай анонімне) спаму на форумах в Інтернеті (при модерації сайтів він може віддалятися з запізненням), на дошках оголошень; спам, пов'язаний з функціонуванням соціальних мереж (навіть якщо користувач в них не зареєстрований) та ін. Якщо користувачі ПЕОМ працюють в організаціях (крім віртуальних), то при підозрі на спам вони зазвичай можуть проконсультуватися з більш досвідченими колегами, звернутися до системного адміністратора. При роботі «на дому» одна і та ж ПЕОМ часто використовується різними особами, включаючи кваліфікованих користувачів і дітей з низьким рівнем ІКТ-компетентності. Проте в Україні засоби типу «батьківського контролю» (для обмеження доступу до сайтів) використовуються рідко. У ряді областей реалізуються спеціальні заходи з навчання людей літнього віку роботі на ПЕОМ (в тому числі і в Інтернеті) для вирішення ними повсякденних завдань. Воно зазвичай включає в себе і формування деяких навичок по боротьбі зі спамом.

Висновки:

– Спам не тільки знижує ефективність використання електронних комунікацій, але й несе безпосередню загрозу інформаційній безпеці організацій та окремих фізичних осіб.

– Широке використання адрес електронної пошти в різних електронних і паперових матеріалах / документах сприяє отриманню їх спамерами з метою подальшого використання.

– Велика кількість ПЕОМ у ВНЗ, специфіка контингенту їх користувачів роблять доцільним прийняття спеціальних заходів захисту від спаму, у тому числі і всередині локальних мереж.

– ІКТ-кваліфікація фахівців і користувачів ПЕОМ дуже важлива для боротьби зі спамом.

Література:

1. Брумштейн, Ю. М. Информационная безопасность использования электронных почтовых ящиков / Ю.М. Брумштейн, Ж. Т. Балбаев, С. В. Пригаро // Информационная безопасность регионов. – 2012. – № 1(10). – С. 13-20.

2. Брумштейн, Ю. М. Анализ факторов информационной безопасности региона и влияния на нее вузов /Ю. М. Брумштейн, Т. Т. Салхенов, С. В. Чернов, А. А. Боркова // Известия ВолГТУ :межвуз. сб. науч. ст. № 12(60) /ВолгГТУ. – Волгоград, 2009. – (Серия «Актуальные проблемы управления, вычислительной техники и информатики в технических системах» ; вып. 7). – С. 99-102.

3. Логинов, В. SMS-спам лишит заключенных связи /В. Логинов // Известия. – 2013. – № 27(28781). – С. 1-4.

4. Набоков, М. В. Создание информационного пространства организации, работающей в быстроизменяющейся среде / М. В. Набоков, О. Н. Ровенская // ИзвестияВолГТУ :межвуз. сб. науч. ст. № 9(82). – Волгоград, 2011. – (Серия «Актуальные проблемы управления, вычислительной техники и информатики в технических системах» ;вып. 11). – С. 88-92.

5. Санжапапов, Б. Х. Модель принятия решений на основе многокритериальной оценки объектов в виде нечетких распределений / Б. Х. Санжапапов, И. С. Калина //Известия ВолГТУ :межвуз. сб. науч. ст. № 8(46) /ВолгГТУ. – Волгоград, 2008. – (Серия «Актуальные проблемы управления, вычислительной техники и информатики в технических системах» ; вып. 5). – С. 76-79.

6. Спам [Електронний ресурс]. – режим доступу : http:// ua.wikipedia.org/wiki/%D1%EF%E0%EC.

7. Сколько спама производит Беларусь? [Електронний ресурс]. – режим доступу : http://naviny.by/rubrics/computer/2013/06/08/ic_articles_128_182003/.

Розглянуто різні визначення спаму. Визначено поняття спаму, його місце у формуванні інформаційного середовища фізичних осіб та організацій, основні його завдання та методи поширення. Проаналізовано вплив спаму на інформаційну безпеку організацій та фізичних осіб. Досліджено методи боротьби зі спамом. Виявлено вплив інформаційно-комунікаційної компетентності користувачів на ефективність боротьби зі спамом. Побудовано математичну модель оцінки збитків, пов'язаних з невірною діагностикою інформації.

Ключові слова: *спам, інформаційна безпека, Інтернет, способи захисту, інформаційно-комунікаційна компетентність.*

Рассмотрены различные определения спама. Определено понятие спама, его место в формировании информационной среды физических лиц и организаций, основные его задачи и методы распространения. Проанализировано влияние спама на информационную безопасность организаций и физических лиц. Исследованы методы борьбы со спамом. Выявлено влияние информационно-коммуникационной компетентности пользователей на эффективность борьбы со спамом. Построена математическая модель оценки убытков, связанных с неверной диагностикой информации.

Ключевые слова: *спам, информационная безопасность, Интернет, способы защиты, информационно-коммуникационная компетентность.*

The different definition of spam. The definition of spam, its place in shaping the information environment of individuals and organizations, its main tasks and methods of distribution. The effect of spam on information security organizations and individuals. Methods of fighting spam. The influence of information and communication competency Users effectiveness against spam. A mathematical model for evaluating losses associated with incorrect diagnosis information.

Key words*: spam, information security, Internet, protection methods, information and communication competence.*

УДК 37.011.3-051:51-057

О.А. Москаленко, Ю.Д. Москаленко, О.В. Коваленко
м. Полтава, Україна

ФОРМУВАННЯ В СТУДЕНТІВ СУБ'ЄКТНОГО ДОСВІДУ ФАХОВОЇ ДІЯЛЬНОСТІ ВЧИТЕЛЯ МАТЕМАТИКИ: ТЕХНОЛОГІЧНИЙ ПІДХІД

Постановка проблеми. Реалізація державної політики у створенні інтелектуального, духовного потенціалу нації, розвитку вітчизняної науки, техніки і культури, загалом, у формуванні людини майбутнього визначається також, з-поміж іншого, і професійністю вчителя.

Як засвідчує практика, модель майбутньої діяльності фахівця формується ще в студентські роки: професійна компетентність учителя математики, рівень готовності математика-педагога до оптимальних дій у контексті конкретних навчальних ситуацій, спрямованих на навчання школярів математики, до використання ефективних технологій організації навчально-пізнавальної діяльності учнів посутньо залежить від того, наскільки сучасною була його підготовка в педагогічному ВНЗ.

Це зумовлює необхідність модернізації системи підготовки вчителя математики, вимагає розробки нових освітніх моделей, зокрема, актуалізує пошук шляхів і засобів створення продуктивних навчальних середовищ, які б поєднували в собі кращі традиції та прогресивні інновації і забезпечували підґрунтя для формування готовності майбутнього фахівця до здійснення професійної діяльності, адекватної сучасним запитам суспільства.

Аналіз попередніх досліджень. Питання фахової підготовки майбутнього вчителя математики завжди були і залишаються в центрі уваги відомих математиків, методистів, викладачів вишів. Теоретичні і практичні аспекти професійної підготовки вчителів-математиків досліджували Г. Бевз, В. Бевз, М. Бурда, О. Дубинчук, В. Моторіна, О. Скафа, С. Семенець, З. Слєпкань та ін. Внесли посутній вклад у розробку засад реалізації компетентнісного підходу в системі підготовки майбутнього вчителя математики І. Акуленко, І. Зимня, О. Матяш, Н. Тарасенкова, В. Швець та ін. Питання вдосконалення й розробки нових педагогічних технологій знайшли відображення в працях А. Вербицького, О. Сидоренка, В. Чуба, (контекстне навчання), О. Осницького, І. Якиманської (формування суб'єктного досвіду особистості) та ін.

Мета статті полягає в обґрунтуванні необхідності створення сучасних інтерактивних навчальних середовищ, орієнтованих на підготовку компетентного вчителя математики, та розкритті особливостей використання пропонованої інтегративної моделі-технології формування в студентів суб'єктного досвіду фахової діяльності вчителя математики.