2. Державний стандарт початкової освіти [Електронний ресурс] – Режим доступу: https://www.kmu.gov.ua/ua/npas/pro-zatverdzhennya-derzhavnogo-standartu-pochatkovoyi-osviti– Назва з екрану. – Дата звернення: 28.10.2018.

3. Концепція Нової української школи [Електронний ресурс]. – Режим доступу: https://www.kmu.gov.ua/storage/app/media/reforms/ukrainska-shkola-compressed.pdf – Назва з екрану. – Дата звернення: 28.10.2018.

4. Морзе Н.В. Проектна діяльність як засіб формування ІКТ компетентності учнів / Н.В. Морзе, О.В. Барна, В.П. Вембер, О.Г. Кузьмінська // Інформатика та інформаційні технології у навчальних закладах. – 2014. – 3 (51). – С 52-59.

5. Пометун О. І. Теорія і практика послідовної реалізації компетентнісного підходу в досвіді зарубіжних країн / О. І. Пометун // Компетентнісний підхід у сучасній освіті: світовий досвід та українські перспективи / під заг. ред. О. В. Овчарук. – К. : К.І.С., 2004. – С. 16-25.

РОЗРОБКА СИСТЕМИ ЗАХИСТУ ВЕБ-СЕРВЕРІВ

Гладій Іван Іванович
магістрант спеціальності «Середня освіта. Інформатика»,
Тернопільський національний педагогічний університет імені Володимира Гнатюка
gladij_ii@fizmat.tnpu.edu.ua

Карабін Оксана Йосифівна
кандидат педагогічних наук,
доцент кафедри інформатики та методики її навчання,
Тернопільський національний педагогічний університет імені Володимира Гнатюка
karabinoksana@gmail.com

Нині веб-сервери підлягають безліччю різноманітних небезпек, де вагому загрозу становлять атаки як хакерів так і вірусів. Перші можуть зламати сайти, отримати доступ до конфіденційної інформації, розміщеної на сервері, внести зміни у їх вміст, а також вивести з робочого ладу сервер за допомогою розподіленої атаки (DDoS-атака). Віруси ж, заражаючи веб-сервери, перетворюють їх у джерело загроз. Крім того, вони істотно сповільнюють роботу серверів, а також змінюють пропускну здатність Інтернет-канал. Первинно розглядають такі загрози за принципом відмінності у їх роботі, але це є не зовсім так. Виявляється, багато вірусів, особливо Інтернет-черв'яки, використовують для поширення уразливості в програмному забезпеченні. Так і хакери використовують такого виду атаки, спрямовані на відомі «дірки» в програмному забезпеченні [2].

Проблема інформаційної безпеки нині набуває стратегічного значення. Практично всі приватні організації мають власний автоматизований банк даних. на думку експертів, витік конфідеційної інформації навіть на 20 % призводить до непоправимих наслідків у роботі таких комерційних фірм [3].

Наукові дослідження показали, що найретельніший захист баз даних приватних організацій і також потребують додаткового захисту системи електронної пошти. У своїх регулярних оглядах веб-серверів служба Netcraft зазначає, що нині служби Інтернету підлягають посиленим атакам, відтак безпека корпоративних сайтів, комерційних серверів, Інтернет сервісів, інформаційних мереж тощо є вразливою та потребують професійного захисту [5]. З практичної сторони в будь-яка програма має вразливості і чим більший її вихідний код за

об'ємом, тим ймовірніше відшукати в ній різних проблемний недоречностей. Їх наявність у коді програми пояснюється тим, що програмісти здатні на помилку. Існує навіть спеціальна норма програмування, в якій зазначено, скільки помилок може допустити фахівець при написанні певного числа рядків коду. Окрім того, не можна забувати, що значне програмне забезпечення розробляється командою фахівців. І досить часто помилки виникають при компонуванні модулів, створених різними програмістами. А також наявність недоречностей далеко не завжди визначається якістю написання програмного забезпечення.

Зважаючи на перераховані проблеми для забезпечення коректної роботи серверів і безпечного доступу до баз даних потрібно звернути увагу на такі особливості як:

– вразливості програмного забезпечення: сьогодні на сайтах, присвячених інформаційній безпеці, постійно з'являються повідомлення про виявлення нових вразливих елементів у програмному забезпеченні. У цьому процесі беруть участь як фахівці з захисту даних, так і хакери.

– вразливості конфігурації: багато проблем з безпекою виникає саме при налаштуванні програмного забезпечення. Безпека сервера сильно залежить від роботи адміністратора, а оскільки це людина, то їй властиво помилятись.

– вразливість власного програмного забезпечення: скрипти веб-сайтів містяться на самому сервері і обробляються також, до користувача надсилаються лиш результаті дій програми. Використання скриптів з вразливими місцями може призвести до несанкціонованого доступу до сервера.

Взявши до уваги проблеми які було розглянуто, можна забезпечити безперебійну роботу серверів і збереження приватних даних. Але багато проблем, пов'язаних із захистом веб-серверів, вимагають ретельного аналізу і опрацьованого рішення, адже на сучасному етапі розвитку інформаційних технологій все більше проявляється залежність ефективного функціонування державних і комерційних підприємств і організацій від безпеки і надійності застосовуваних корпоративних інформаційно-телекомунікаційних систем. Серед основних вимог, що пред'являються до таких систем, можна виділити необхідність забезпечення послуги доступності. Через те, що одним з найпоширеніших видів атак у сучасних мережах є атаки типу відмови в обслуговуванні, які при успішній реалізації здатні паралізувати роботу як окремих серверів, так і цілих мереж, проблема забезпечення доступності ресурсів є надзвичайно актуальною для загальнодоступних інформаційних систем, у зокрема, мережі Інтернет.

Список використаних джерел:

1. DDoS and Security Reports: The Arbor Networks Security Blog: веб-сайт. URL: https://threathub.arbornetworks.com. (дата звернення: 15.5.2018).

2. Сайт Лаборатории Касперского: веб-сайт. URL: https://www.kaspersky.com. (дата звернення: 15.5.2018).

3. Олифер В. Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы / Олифер В. Г., Олифер Н.А. 4 издание, 2010, 943с.

4. Статистика глобальной сетевой активности: веб-сайт. URL: https://www.web-canape.ru/business/socialnye-seti-v-2018-godu-globalnoe-issledovanie. (дата звернення: 15.5.2018).

5. Abliz M. Internet Denial of Service Attacks and Defense. Pittsburgh : University of Pittsburgh Technical Report: веб-сайт. URL: https://www.mathematics.pitt.edu/research /technical-reports. (дата звернення: 16.5.2018).

ТЕХНОЛОГІЯ «ВЕБ-КВЕСТ» ЯК ЗАСІБ РЕАЛІЗАЦІЇ КОМПЕТЕНТНІСТНОГО ПІДХОДУ В НАВЧАННІ МАТЕМАТИКИ

Гоменюк Ганна Володимирівна
кандидат педагогічних наук,
асистент кафедри математики та методики її навчання,
Тернопільський національний педагогічний університет імені Володимира Гнатюка
anita.homenyuk@gmail.com

Одним із завдань впровадження компететнісного підходу в шкільну математичну освіту є формування в учнів інформаційно-цифрової компетентності, що передбачає розвиток умінь «структурувати дані, діяти за алгоритмом та складати алгоритми, визначати достатність даних для розв'язання задачі, використовувати різні знакові системи, знаходити інформацію та оцінювати її достовірність, доводити істинність тверджень» [4, с. 5]. Інформаційно-цифрова компетентність має забезпечити в процесі навчання математики становлення критичного осмислення школярами інформації та джерел її отримання, усвідомлення важливості ІКТ для ефективного розв'язування, зокрема, математичних задач.

Веб-квест – це сучасна технологія, яка заснована на проектному методі навчання, що включає пошукову діяльність учнів разом з учителем в мережі Інтернет. Найхарактернішою ознакою такого способу пізнання є те, що кожний школяр долучається до співпраці в команді, а учень і вчитель стають рівноправними суб'єктами навчально-виховного процесу. Під час такого спільного пошуку здійснюється обмін думками, знаннями, способами діяльності, забезпечується об'єктивне оцінювання здобутих результатів [2].

Технологія веб-квест дозволяє ефективно формувати не лише інформаційно-цифрову компетентність, а й інші компетентності: комунікаційну компетентність (робота в команді, планування, розподіл функцій, взаємодопомога, взаємоконтроль); математичну компетентність (уміння знаходити декілька способів розв'язку задачі, визначати найбільш раціональний варіант розв'язку) та інші.

Веб-квест повинен включати в себе наступні структурні компоненти [3].

Вступ, де чітко описані головні ролі учасників або сценарій квесту, попередній план роботи, огляд усього квесту.

Центральне завдання, яке є зрозумілим та цікавим.

Список інформаційних ресурсів, необхідних для виконання завдання.

Опис процедури роботи, яку необхідно виконати кожному учаснику.

Опис критеріїв та параметрів оцінювання результатів веб-квесту.

Вимоги до презентації зібраної інформації.