

УДК 004.891.3

## МЕТОДИ І АЛГОРИТМИ ЗАХИСТУ ІНФОРМАЦІЇ У WEB-ОРІЄНТОВАНИХ СИСТЕМАХ ДИСТАНЦІЙНОГО ДІАГНОСТУВАННЯ РІВНЯ ЗНАНЬ

**Ю. В. Безгачнюк**

*Івано-Франківський національний технічний університет нафти і газу;  
76019, м. Івано-Франківськ, вул. Карпатська, 15;  
тел. +380 (3422) 4-80-00; e-mail: [yurkovskiy@gmail.com](mailto:yurkovskiy@gmail.com)*

*В статті розглянуто методи і алгоритми захисту інформації у Web-орієнтованих системах дистанційного діагностування рівня знань, а також наводиться реалізація відповідного апарату в системі d-tester, яка використовується на кафедрі КТіСУ ІФНТУНГ.*

**Ключові слова:** захист інформації, діагностування рівня знань, комп'ютерне тестування.

### **Вступ**

На сьогоднішній день великої популярності досягла дистанційна форма навчання. Для цього використовуються сучасні засоби обчислювальної техніки, а, особливо, засоби і сервіси, які надає всесвітня мережа Інтернет. Web-орієнтовані системи діагностування рівня знань, а також окремі модулі, які складовими систем дистанційного навчання, як і будь-яка web-орієнтована інформаційна система не позбавлена проблем, пов'язаних із безпекою.

Програмно-технічні методи і засоби є технічною основою систем захисту інформації. Застосування таких засобів здійснюється структурними органами у відповідності з прийнятою політикою інформаційної безпеки, як описана в нормативно-методичних документах.

Для того, щоб сформувати оптимальний комплекс (набір) програмно-технічних методів і засобів захисту інформації, необхідно пройти такі етапи:

- визначення інформаційних і технічних ресурсів, які підлягають захисту;
- виявлення повної множини потенційно можливих загроз і каналів витоку інформації;
- проведення оцінки вразливості і ризиків інформації при існуючій множині загроз і каналів витоку;
- визначення вимог до системи захисту;
- здійснення вибору засобів захисту інформації і їх характеристики;
- впровадження і організація використання вибраних заходів, способів і засобів захисту;
- здійснення контролю цілісності і управління системою захисту.

До системи захисних методів і засобів входять програмні методи, апаратні засоби, захисні перетворення, а також організаційні заходи. На рис. 1 показаний склад захисних методів і засобів [1].

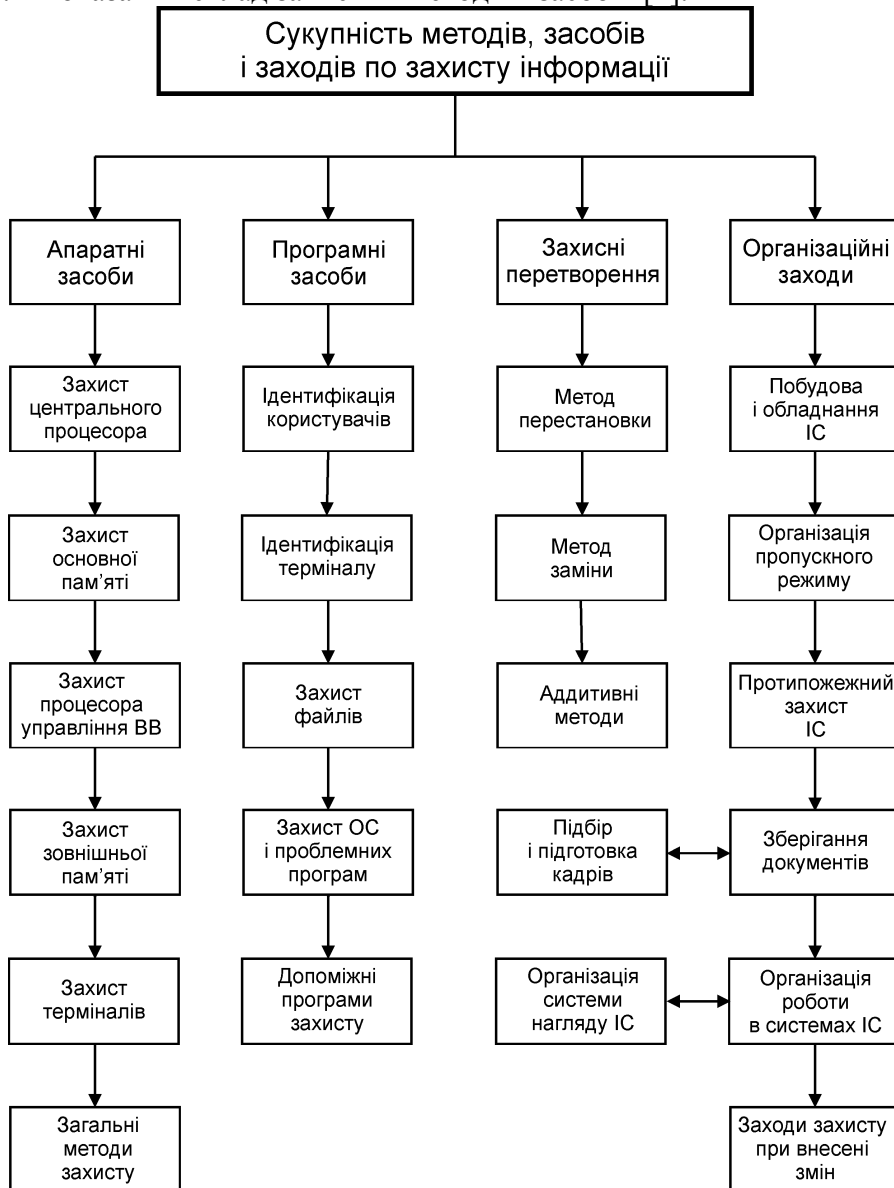


Рис. 1. Сукупність методів, засобів і заходів з захисту інформації

Сутність апаратного або схемного захисту полягає в тому, що в пристроях і технічних засобах обробки інформації передбачається наявність спеціальних технічних рішень, що забезпечують захист і контроль інформації, наприклад екрануючі пристрої, які локалізують електромагнітні випромінювання або схеми перевірки інформації на парність, яка здійснює контроль за правильністю передачі інформації між різними пристроями ІС.

Програмні методи захисту – це сукупність алгоритмів і програм, що забезпечують розподіл прав доступу і виключають несанкціоноване використання інформації.

Сутність методів захисних перетворень полягає в тому, що інформація, яка зберігається в системі і передається каналами зв'язку, подається у певному коді, що виключає можливість її безпосереднього використання.

Лише комплексне використання різного роду захисних заходів може забезпечити надійний захист, так як кожний прийом або метод має свої слабкі і сильні сторони.

З точки зору програмної реалізації неможливо охопити апаратні засоби і організаційні заходи щодо захисту інформації, тому, в даній статті буде розглянуто лише програмні засоби і захисні перетворення, які в більшості випадків виступають разом, а не окремо.

Використання web-орієнтованих інформаційних систем передбачає обмін інформацією між клієнтом і сервером, що в більшості випадків реалізується за допомогою HTML-форм. Для систем дистанційного оцінювання рівня знань це переважно такі управляючі елементи, як: радіо-кнопки, поля для вводу, прапорці і списки вибору. При передачі інформації на сервер, в атрибутах вище перелічених управляючих елементів передається службова інформація. При аналізі деяких популярних систем дистанційного навчання і комп'ютерного тестування з використанням Web, було виявлено значні недоліки в реалізації алгоритмів генерації форм з точки зору безпеки, а саме в атрибуті управляючих елементів містилась службова інформація, яка давала змогу частково, а в деяких випадках і повністю, дати правильну відповідь на те чи інше завдання, що є неприпустимим [2].

Для вирішення даної проблеми в системі дистанційного діагностування рівня знань студентів d-tester використовується метод заміни значень службових ідентифікаторів. Суть даного методу полягає в наступному:

- на форму управляючі елементи поміщуються із значеннями службових атрибутів у строгій послідовності (1, 2, 3, 4 ... n);
- реальні значення зберігаються в масиві, який розміщений у файлі (сховищі) сеансу, який для кожного користувача генерується окремо.

Алгоритм роботи методу заміни значень службових ідентифікаторів працює так:

- варіанти відповідей на деякі завдання у файлі (сховищі) сеансу зберігаються у структурах, імена яких мають такий формат `ans_<номер_завдання>_<номер_варіанту_відповіді>`;

- генерується масив із послідовними значеннями номерів варіантів відповідей для даного завдання ([індекс]=>значення)

```
ans_num = Array ([0]=>1 [1]=>2 [2]=>3 [3]=>4 [4]=>5 [5]=>6 )
```

- елементи масиву випадково переміщуються по масиву (змінюється індекс елемента);

```
ans_num = Array ([0]=>3 [1]=>5 [2]=>1 [3]=>4 [4]=>2 [5]=>6 )
```

- при генеруванні HTML-форми значення службових атрибутів для управляючих елементів вибираються із значень індексів масиву `ans_num`, тобто є завжди послідовними (для вище наведеного прикладу 0 ... 5;

- аналіз відповіді користувача відбувається шляхом визначення значення елемента масиву `ans_num` у відповідності до вибраного індексу користувача;

- згідно із внутрішнім представленням варіантів відповідей на тестові завдання в системі `d-tester`, для подальшої обробки використовуються вже значення елементів масиву `ans_num` для подальшої перевірки вибраного варіанту.

При використанні мультимедіа ресурсів у варіантах відповідей для завдань закритого типу, існує можливість ідентифікувати правильний / неправильний варіант за назвою ресурсів, яка не змінюється і є сталою. Мультимедіа ресурс поміщується на HTML-сторінку шляхом використання деякого контейнера (наприклад `<img>`) із вказуванням атрибуту, в якому записується шлях до файлу деякого ресурсу [2].

Для вирішення цієї проблеми в системі `d-tester` використовується алгоритм заміни шляху до файлу ресурсу.

Алгоритм працює наступним чином:

- генерується деяка випадкова послідовність;
- генерується значення хеш-функції від попередньо згенерованої випадкової послідовності;
  - значення хеш-функції є індексом елемента масиву, значенням якого є реальний шлях до файлу;
  - при виведенні зображення на HTML-сторінку викликається проміжний сценарій, в який передається значення хеш-функції, відповідно, у файлі сценарію згідно переданого значення визначається реальний шлях до файлу шляхом аналізу вмісту елемента масиву із відповідним індексом.

Використання описаних вище простих алгоритмів заміни підвищує об'єктивність оцінювання рівня знань осіб, котрі навчаються, що і є головною метою використання подібних систем.

### *Література*

1. Домарев В. Защита информации и безопасность компьютерных систем [Текст] / В. Домарев. – К.: "ДиаСофт", 2005. – 672 с.
2. Безгачнюк Ю. В. Проблеми захисту інформації в Web-орієнтованих системах дистанційного діагностування рівня знань / Ю. В. Безгачнюк // Наукові вісті інституту менеджменту та економіки "Галицька Академія". – 2009. – №1. – с. 32-35. – Бібліограф.: с. 35.

*Стаття надійшла до редакційної колегії 24.12.2010 р.*

*Рекомендовано до друку д.т.н., професором Заміховським Л.М..*

---

---

**METHODS AND ALGORITHMS FOR DATA PROTECTION IN  
WEB-ORIENTED SYSTEMS OF DISTANCE DIAGNOSTICS OF  
KNOWLEDGE'S LEVEL****Y. V. Bezgachnyuk***Ivano-Frankivs'k National Technical University of Oil and Gas;**76019, Ivano-Frankivs'k, st. Carpats'ka, 15;**ph. +380 (3422) 4-80-00; e-mail: [yurkovskiy@gmail.com](mailto:yurkovskiy@gmail.com)*

*This article describes methods and algorithms for data protection in Web-oriented systems of distance diagnostics of knowledge's level. Also provides the implementation this algorithms in d-tester system, which is used at the department KTSU IFNTUOG*

**Keywords:** *data protection algorithms, web-oriented systems of distance diagnostics of knowledge's level*