ІНФОРМАЦІЙНА БЕЗПЕКА

УДК 004.056:371.26:378.14

Н. П. Кухарська, *канд. фіз.-мат. наук, доцент*
(Львівський державний університет безпеки життєдіяльності)

РОЗРОБКА ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНОГО КОНТРОЛЮ ЗНАНЬ

У статті розроблено політику інформаційної безпеки використання комп'ютерних систем перевірки знань. З'ясовано, яка інформація циркулює у межах цих систем, виявлено загрози, ідентифіковано атаки, побудовано модель порушника та вироблено набір вимог, правил, обмежень, рекомендацій, які регламентують процес тестування і спрямовані на захист інформації. Неухильне дотримання усіма користувачами вимог політики інформаційної безпеки сприятиме досягненню і підтримці стану інформаційної захищеності системи комп'ютерного контролю.

Ключові слова: комп'ютерний контроль знань, комп'ютерне тестування, автоматизована система перевірки знань, політика інформаційної безпеки, загроза, атака, модель порушника.

N. P. Kukharska

DEVELOPMENT OF INFORMATION SECURITY POLICY OF COMPUTER KNOWLEDGE CONTROL

The article describes the information security policy for using computer knowledge verification systems. Nature of information, circulating within these systems has been determined, threats have been found, attacks have been identified, an attacker's abstract model has been constructed and a set of requirements, rules, restrictions, recommendations regulating the process of testing and aiming information protection have been made. Accurate compliance the requirements of information security policy by all users will contribute to the achievement and maintenance of the state of information security of the computer control system.

Keywords: computer knowledge control, computer testing, automated knowledge validation system, information security policy, threat, attack, attacker's abstract model**.**

Вступ. Сьогодні, у період реформування освіти, що супроводжується зменшенням обсягу аудиторних занять та збільшенням за їх рахунок кількості годин, відведених на самостійну роботу, педагогічний контроль як засіб діагностики рівня засвоєння студентами теоретичного матеріалу, формування вмінь й навичок набуває все більшої ваги.

Навчальний процес не може бути ефективним без систематичного оцінювання результатів навчання, основною функцією якого є забезпечення зворотного зв'язку. Аналізуючи отримані студентами оцінки, викладач має змогу з'ясувати чи досягнута на певному етапі освітнього процесу навчальна мета і, відповідно до зробленого висновку, виробити подальшу стратегію управління навчально-пізнавальною діяльністю студентів.

Кожний, без винятку, із застосовуваних викладачами методів і форм контролю навчальних досягнень студентів має свої переваги і недоліки, свої обмеження. Так, основним недоліком таких традиційних форм контролю, як письмова контрольна робота, лабораторна робота, усне опитування, курсова робота, дипломна робота, реферат, співбесіда, тощо є суб'єктивність, тобто залежність оцінки знань студента від думки людини, яка перевіряє. Мінімальним втручанням викладача характеризується тестова форма контролю.

Розрізняють такі види перевірки знань у вигляді тестів [1]:

- *Бланкове тестування (типу "paper-and-pencil").* При такому підході для контролю знань використовують заздалегідь підготовлені бланки, що містять контрольні завдання (тести).

▪ *Контроль знань з використанням технічних пристроїв.* Студент, отримує від викладача індивідуальний набір завдань, виконавши їх, вводить у пристрій номер свого варіанта, результати розв'язання завдань. Пристрій перевіряє введені відповіді і виводить оцінку за роботу.

▪ *Комп'ютерний контроль знань.* Його забезпечують спеціальні комп'ютерні програми, які:

– формують індивідуальний набір контрольних завдань кожному опитуваному;
– виводять завдання на екран;
– аналізують відповіді;
– виставляють оцінки;
– зберігають результати контролю і дані про роботу студента, котрі згодом можуть бути використані викладачем.

▪ *Віддалений контроль знань.* Це різновид комп'ютерного контролю, що передбачає використання мережі Internet. Характерними рисами віддаленого контролю знань є застосування сучасних технічних засобів зв'язку для передачі інформації між студентом і викладачем.

У статті розглянемо комп'ютерний контроль знань.

Постановка проблеми. Створюючи спеціальне програмне забезпечення для проведення тестувань, розробники дбають про зручний графічний інтерфейс, переймаються способами збереження тестів і відповідей на них, слідкують за тим, наскільки широко представлені різні типи використовуваних завдань. В один момент усі ці старання можуть звестися нанівець, якщо дадуться взнаки огріхи, що стосуються забезпечення інформаційної безпеки. Недопрацювання у цьому напрямку розробників автоматизованої системи тестування, недбале ставлення до вирішення питань інформаційної безпеки її користувачів можуть призвести до компрометації як окремих результатів тестування, так і всієї системи в цілому.

Проводячи комп'ютерне тестування, викладач має на меті оперативно отримати об'єктивну оцінку знань. У той же час, ціллю студента є одержати максимально можливі бали за тест. Не виключено, що у студента може з'явитися бажання вплинути на результати тестування. Він намагатиметься знайти прогалини системи комп'ютерного тестування, що пов'язані із безпекою інформації та скористатися ними. Щоб звести до мінімуму результативність таких намагань, необхідно розробити та впровадити політику інформаційної безпеки, зміст якої слід довести до відома усіх користувачів автоматизованої системи тестування знань.

Виклад основного матеріалу. Розроблення політики інформаційної безпеки передбачає виявлення загроз, у нашому випадку, комп'ютерної системи перевірки знань, ідентифікацію атак, побудову моделі порушника та вироблення набору вимог, правил, обмежень, рекомендацій, які регламентуватимуть порядок інформаційної діяльності, пов'язаної з використанням цієї автоматизованої системи. Дотримання політики інформаційної безпеки усіма користувачами має сприяти досягненню і підтримці стану інформаційної захищеності системи комп'ютерного контролю знань.

Під захищеністю системи комп'ютерного контролю знань будемо розуміти ступінь адекватності реалізованих у ній механізмів захисту інформації наявним у цьому середовищі функціонування ризикам, які пов'язані із загрозами безпеці інформації.

Загроза безпеці інформації – будь-які обставини чи події, що можуть спричинити порушення таких властивостей інформації, як конфіденційність, цілісність і доступність.

Конфіденційність (confidentiality) – властивість, яка вказує на недоступність інформації чи сервісів інформаційної системи для користувача, якому апріорно не надана можливість використання зазначених сервісів або інформації.

Цілісність (integrity) – властивість збереження повноти і точності інформації.

Доступність (availability) – властивість, яка вказує на можливість авторизованого користувача використовувати інформацію та ресурси інформаційної системи у потрібний момент часу відповідно до правил, встановлених політикою безпеки.

З'ясуємо, яка інформація циркулює у середовищі автоматизованої системи перевірки знань.

Такою інформацією є:

- тестові завдання;
- варіанти відповідей на них з виокремленням правильних;
- відповіді студентів на тестові завдання;
- результати перевірки у вигляді оцінки за певною шкалою.

Основними загрозами порушення конфіденційності, цілісності, доступності цієї інформації є: несанкціонований доступ, знищення, модифікація, витік інформації, порушення роботи, у тому числі блокування, автоматизованої системи перевірки знань.

Опишемо найбільш ймовірні атаки, за допомогою яких реалізовуються визначені вище загрози:

- підказки з боку осіб, що не проходять тестування (викладача, системного адміністратора, контролюючої особи), а також з боку інших студентів, які тестуються у той же час;
- підміна під час тестування одного студента іншим;
- підглядування відповідей у сусіда;
- списування з паперових та електронних шпаргалок;
- пошук відповідей у мережі Інтернет;
- атака на дані, що передаються лініями зв'язку.

Як було зауважено, розроблення політики інформаційної безпеки передбачає побудову моделі порушника.

Модель порушника (attacker's abstract model) – це абстрактний формалізований (або неформалізований) опис вірогідних дій порушника, який складається на основі аналізу його типу, рівня повноважень, знань, теоретичних та практичних можливостей.

Загрозу інформаційній безпеці комп'ютерної системи тестування знань можуть становити внутрішні і зовнішні порушники. До внутрішніх віднесемо фахівців, які обслуговують цю комп'ютерну інформаційну систему та користувачів (викладачів і студентів). Вони можуть завдати шкоду як навмисно, так і ненавмисно. Зовнішні порушники – це сторонні особи, які перебувають поза вищим навчальним закладом або неавторизовані для використання цієї комп'ютерної системи (КС). Це означає, що вони не мають в КС облікового запису і згідно із системною політикою безпеки взагалі не можуть працювати у ній. Приклад зовнішніх порушників – кваліфіковані хакери.

За місцем дії можна виокремити кілька типів порушників:

- порушник перебуває поза територією вищого навчального закладу;
- порушник діє на території вузу без доступу до приміщень, де розташована і функціонує КС;
- порушник перебуває на території вузу, усередині приміщень, але без доступу до технічних засобів КС;
- порушник має доступ до робочих місць користувачів КС;
- порушник має доступ до інформації (баз тестових завдань, архівів і т.ін.) КС;
- порушник має доступ до управління засобами забезпечення безпеки інформації, що циркулює в КС.

За характером дій порушників можна класифікувати так [2]:

- "випадковий порушник", що помилково, ненавмисно і несвідомо порушив політику безпеки КС у процесі виконання своїх посадових обов'язків (системний адміністратор, викладач) чи в процесі проходження тестування (студент);

– “терплячий порушник” безпеки, що порушив політику безпеки свідомо, навмисно, але без рішучих дій, маскуючись, підбираючи атрибути доступу легітимних користувачів з метою подолання засобів управління доступом тощо;
– “рішучий зловмисник”, який має на меті порушити одну із властивостей інформації, що циркулює в КС. Він прагне подолати наявні засоби обмеження доступу і отримати можливість безпосереднього доступу до інформації з метою втручання у роботу КС, модифікації, знищення чи отримання необхідної інформації;
– “віддалений порушник”, що аналізує технічні канали витоку інформації, впливає на локальні та розподілені мережі КС віддалено за допомогою спеціальних засобів, включаючи технології VPN, Wi-Fi, WiMAX тощо.

Сформулюємо рекомендації, правила, дотримання яких дасть змогу досягти і підтримувати стан інформаційної захищеності системи комп’ютерного тестування знань.

- Тестування слід проводити у контрольованому приміщенні.
- У програмі, що застосовується для тестування, має бути впроваджена система розмежування прав доступу, яку, як правило, реалізовують на основі парольної аутентифікації. Кожному зареєстрованому користувачеві, що має персональні логін і пароль, системний адміністратор надає відповідні права доступу до інформаційних ресурсів та функцій програми.
- Системний адміністратор зобов’язаний забезпечити блокування облікових записів користувачів автоматизованої системи тестування знань у таких випадках:
  – п’яти поспіль невдалих спроб автентифікації (автоматичне блокування);
  – завершення студентом навчання у вузі;
  – звільнення з роботи викладача.
- Потрібно зобов’язати користувачів здійснювати безпосередній вихід із комп’ютерної системи тестування знань після закінчення роботи з нею.
- Щоб запобігти підміні одного студента іншим, викладачеві слід додатково проводити аутентифікацію студентів візуально. Викладач, який читає лекції великій аудиторії, може не пам’ятати персонально всіх студентів, водночас він повинен бути впевненим, що студент, який проходить тестування є тим, за кого себе видає. Одним з можливих варіантів вирішення цього питання є перевірка залікової книжки або студентського квитка. Що стосується віддаленого тестування, то, на жаль, нейтралізувати загрозу підміни одного студента іншим неможливо.
- Студенти, які сидять поруч, на моніторі мають бачити різні тестові завдання. Досягається це шляхом рандомізації порядку слідування як варіантів відповідей в рамках одного тестового завдання, так і самих тестових завдань в рамках тесту.
- Генерація пакета завдань для кожного студента має здійснюватися шляхом випадкової їх вибірки з відповідної бази. У той же час, тестових завдань у базі мало би бути доволі багато. Тоді рідше будуть повторюватися питання у пакетах, автоматично сформованих системою для різних студентів. А чим менша ймовірність повторення завдань, тим об’єктивніші результати тестування знань студентів. Зауважимо, використання комп’ютерів, як сховища інформації великих обсягів, створює сприятливі умови для розширення тестової бази.
- Необхідно постійно оновлювати базу тестових завдань. І йдеться тут уже не стільки про кількісне її доповнення, як про якісну видозміну. Тобто, слід час від часу змінювати формулювання завдань, використовуючи інші мовні звороти. Це дасть змогу уникнути масових списувань зі шпаргалок.
- Комп’ютерне тестування потрібно проводити для всіх студентів однієї академічної групи одночасно.
- Щоб не було списувань з електронних шпаргалок, щоб студенти, тестуючись, не змогли зберегти, наприклад, засобами будь-якого текстового редактора завдання і розповсюдити їх опісля, необхідно заборонити користуватися під час тестування переносними носіями інформації.

- Також, з описаних вище причин, рекомендується на час сеансу тестування відключити доступ до інформаційних ресурсів мережі Інтернет.
- Використання комп'ютерної програми перевірки знань загалом та адміністрування тестів зокрема не повинні вимагати від викладача досвіду роботи з іншими програмами. Важливість виконання цієї вимоги є очевидною: кожний викладач буде здатний самостійно створити тест, у нього відпаде потреба звертатися за допомогою до сторонніх осіб, що знизить ймовірність витоку інформації – тестових завдань.

Для ефективного використання програми розробниками мала б бути також передбачена можливість вносити зміни у тести безпосередньо у програмі. Це нескладно реалізувати, впровадивши у робоче середовище комп'ютерної програми тестування знань окреме вікно, у якому можна: ввести нове тестове завдання, варіанти відповідей, позначити правильну відповідь, зберегти, а у разі потреби модифікувати раніше внесені тестові завдання.

- Бажаною є повна автоматизація процесу тестування. Тестування має відбуватися без втручання викладача. Весь процес від формування пакета тестових завдань, проходження тестування до оцінювання результатів, – повинен проходити для усіх студентів за єдиним сценарієм, без можливості викладача, студента чи ще будь-кого вплинути на хід його виконання. Результатом тестування має бути відомість по групі і у разі потреби – повний звіт з відповідями на тестові завдання по кожному студентові.
- Базу тестових завдань бажано організувати у вигляді окремого блоку, який слід зберігати на іншому (не на тому, на якому розташовується сама система тестування знань) захищеному сервері. Користувач підключатиметься до сервера за допомогою клієнтської програми, якою може бути будь-який встановлений на комп'ютері Інтернет-браузер. Всі дані мають братися і передаватися на сервер без дублювання на комп'ютері користувача. Це перешкоджатиме несанкціонованому доступу до бази завдань з боку студентів, інших сторонніх осіб, читанню тестових запитань та правильних відповідей, розповсюдженню їх серед студентської аудиторії.
- Категорично не рекомендується застосування користувачами функції "запам'ятовування пароля" веб-браузера, з якого здійснюється вхід до автоматизованої системи тестування знань.
- Варто ввести часове обмеження на проходження тесту. Це можна реалізувати двома способами. Перший спосіб – можна лімітувати час відповіді на тестове завдання. Після закінчення цього терміну програма автоматично переходить до наступного тестового завдання. Інший спосіб – це обмеження у часі всього процесу тестування. У цьому випадку студент має можливість самостійно розподіляти час для виконання кожного тестового завдання.

Деякі автори [3,4] рекомендують дозволити студентам під час тестування використовувати підручники. Обмеження по часу, на їх думку, не дасть змоги скористатися підручниками у повній мірі. Водночас, такий дозвіл, як вони вважають, буде стимулювати студентів читати рекомендовану викладачем літературу.

- Слід передбачити резервне копіювання електронної бази тестових завдань та бази результатів тестувань з метою можливості відновлення їх у разі виникнення апаратно-програмних збоїв та інших нештатних ситуацій. Реалізація гнучкої системи резервного копіювання, у тому числі вибір оптимальної (щомісячної/щотижневої/щоденної) частоти резервування, забезпечить надійність комп'ютерного тестування.
- Щоб забезпечити збереження конфіденційності даних під час інформаційного обміну між сервером і користувачами, необхідно максимально захистити їх передавання лініями зв'язку, використовуючи процедури шифрування на основі криптографічних алгоритмів високої стійкості.

Висновки. Інформаційні технології, впроваджені в навчання, допомагають досягти запланованих результатів лише за умови виваженого і продуманого підходу до їх застосування.

На основі особистого багаторічного досвіду використання тестової підсистеми платформи Moodle робимо висновок: комп'ютерне тестування з дотриманням вимог політики ін-

формаційної безпеки дає змогу помітно покращити освітній процес. У той же час, ми не бачимо потреби цілком відмовлятися від традиційних форм опитування, оскільки переконані, що жодне тестування не замінить педагогічний досвід та індивідуальний внесок кожного викладача. На нашу думку, для ефективного контролю знань студентів слід використовувати як комп'ютерне тестування, так і традиційні форми опитування, вміло поєднуючи їх. Вважаємо, що основними завданнями комп'ютерного тестування є допомогти викладачеві організувати систематичний, багатоступінчастий контрольно-оцінювальний процес і у такий спосіб створити сприятливі умови для активізації пізнавальної діяльності студентів.

Список літератури:

1. Молчанова О. Г. Интеграция информационных технологий в системах удаленного контроля знаний в вузах в единую информационную систему / Молчанова О. Г., Соколов А. Ю. // Системи обробки інформації. – 2012. – Вип. 3, Т. 1. – С. 179-185.

2. Методи перехоплення інформації у системах квантової криптографії / Горбенко І. Д., Іванченко Є. В., Карпенко С. В., Гнатюк С. О. // Захист інформації. – 2011, № 2. – С. 5-13

3. Андронатій П. І. Комп'ютерні технології в освітніх вимірюваннях : навч.-метод. посібник / Андронатій П. І., Котяк В. В. – Кіровоград : Видавець Лисенко В.Ф., 2011. – 144 с.

4. Морев И. А. О защите качества в системе открытого образования. Опыт массовых тестирований студентов и неожиданные проявления образовательной специфики // Морев И. А., Вовна В. И. // Единая образовательная информационная среда: проблемы и пути развития : III Всерос. научн.-практ. конф.-выставка, г. Омск, 14-17 сентября 2004 г. : материалы. – Омск : Изд-во ОмГУ, 2004. – С. 298-299.

References:

1. Molchanova, O. H., & Sokolov A. Yu. (2012). Integration of information technologies in systems of remote control of knowledge in higher educational institutions into a single information system. *Systemy obrobky informatsii (Systems of information processing),* 3,1, 179-185 (in Russ.)

2. Horbenko, I. D., Ivanchenko, Ye. V., Karpenko, S. V., Hnatiuk, S. O. (2011). Methods of interception of information in systems of quantum cryptography. *Zakhyst informatsii (Protection of information),* 2, 5-13 (in Ukr.).

3. Andronatii, P. I., & Kotiak, V. V. (2011). *Computer technologies in educational measurements.* Kirovograd: Publisher Lysenko, V. F., 144 (in Ukr.).

4. Moriev, I. A., & Vovna, V. I. On quality protection in the open education system. The experience of mass student testing and unexpected manifestations of educational specifics. (2004, 4-17 September). *Unified educational information environment: problems and development paths.* Omsk: Publishing OSU, 298-299 (in Russ.)

❖❖❖