В. Г. Головань,
кандидат технічних наук, професор,
завідувач кафедрою інформаційної безпеки
факультету комп'ютерних наук та інноваційних технологій,
Міжнародний гуманітарний університет
В. В. Сергєєв,
кандидат технічних наук, доцент,
доцент кафедри інформаційної безпеки
факультету комп'ютерних наук та інноваційних технологій,
Міжнародний гуманітарний університет
В. Н. Герасимов,
старший викладач кафедри інформаційної безпеки
факультету комп'ютерних наук та інноваційних технологій,
Міжнародний гуманітарний університет

ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМ ДИСТАНЦІЙНОГО НАВЧАННЯ

Дистанційне навчання (ДН) отримало широке застосування у світовій освітній практиці, що обумовлено його доступністю, масовістю і розвитком засобів телекомунікації, обчислювальної техніки.

В Україні проблема дистанційного навчання також набуває актуальності у зв'язку з потребою в масовій підготовці і перепідготовці кадрів для адаптації до умов ринкової економіки. Відповідно до закону України «Про вищу освіту» ДН, нарівні з іншими формами навчання, набуло офіційного статусу самостійної форми навчання і є однією з форм безперервного навчання [1].

Інформаційно-освітнє середовище ДН являє собою системно-організовану сукупність засобів передачі даних, інформаційних ресурсів, протоколів взаємодії, апаратно-програмного й організаційно-методичного забезпечення, орієнтованих на задоволення освітніх потреб користувачів. Можна виділити наступні фактори та процеси, що призводять до необхідності та доцільності використання ДН:

- високі вимоги до освіти (доступність, невисока вартість навчання, відсутність обмежень по часу навчання та ін.);
- поява і розвиток якісно нових засобів інформаційних технологій (ІТ) і яскраво виражений процес інформатизації;
- підвищення кількості бажаючих отримати освіту через підвищення престижу освіти;
- обмеження по пропускній здатності вузів, факультетів підвищення кваліфікації та освітніх установ інших типів;
- посилення міжнародної інтеграції та ін.

Інформація, що циркулює в системі дистанційного навчання (СДН), повинна бути надійно захищена від знищення, модифікації, підміни, копіювання, несанкціонованого доступу і блокування.

До проблем забезпечення безпеки, які виникають при створенні та експлуатації СДН, можна віднести:

- реєстрацію та автентифікацію користувачів;
- розмежування доступу до інформації;
- захист цілісності, конфіденційності та доступності інформації, в тому числі переданої по відкритих каналах зв'язку;

• забезпечення надійної і коректної роботи компонентів СДН;
• забезпечення інформаційної безпеки баз даних;
• забезпечення безпеки і достовірності системи оплати рахунків.

Проаналізуємо більш детально шляхи вирішення перших двох проблем і розглянемо деякі методи захисту інформації, пов'язані з ними.

Методи реєстрації і автентифікації залежать від систем автентифікації/ ідентифікації, що застосовані у конкретній СДН.

На даний момент отримали розвиток наступні засоби автентифікації/ ідентифікації користувачів:

• програмні (паролі, компоненти програмного забезпечення (ПЗ) та ін.);
• технічні (смарт-картки, електронні ключі типу iButton (таблетки пам'яті) і т. п.);
• біометричні (сканери сітківки ока, відбитки пальця, долоні, індивідуальні особливості голосу, клавіатурного почерку та ін.)

Перераховані системи розрізняються своєю вартістю, складністю реалізації, часом реєстрації нового користувача і автентифікації або ідентифікації, ймовірністю помилкового прийняття законного користувача за порушника, і навпаки. Їх застосовність також залежить від необхідності особистої реєстрації користувача в навчальному закладі. Наприклад, пароль можна передати по електронній пошті, а ось смарт-картку передати по віртуальному простору неможливо.

Застосування смарт-карток, таблеток пам'яті, біометричних засобів вимагає введення спеціального зчитувального обладнання. Останнім часом пристрої зчитування відбитку пальця вбудовують в маніпулятор-мишу, а сітківка ока може розпізнаватися за допомогою web-камери.

При нинішньому розвитку обчислювальної техніки паролі стали ненадійними і часто зламуються. Зате використання біометричних параметрів людини таких, як голос або клавіатурний почерк, являє собою надійний і недорогий спосіб ідентифікації користувачів.

Для ідентифікації по голосу необхідна наявність звукової плати, і, принаймні, мікрофона, тобто робоча станція повинна бути забезпечена мультимедіасистемою. При розпізнаванні по клавіатурного почерку додаткового обладнання не треба, достатньо стандартної клавіатури.

Існує ще одне рішення, завдяки якому сама процедура автентифікації стає прозорою для користувача: коли СДН будується на клієнт-серверній архітектурі. Програма-сервер зберігає лекції, лабораторні заняття, надає доступ до них і перевіряє виконані завдання. Користувач отримує по електронній пошті або на компакт-диску клієнтську частину даного програмного забезпечення. Тільки її власники можуть зв'язуватися і працювати з серверною частиною, причому в кожну програму вшита деяка унікальна для кожного користувача системи послідовність даних, іменована далі ключем, що дозволяє вирішувати відразу кілька проблем захисту інформації.

На основі ключа проводиться автентифікація програми, яка зв'язалася з сервером. За допомогою ключа реалізується як симетричне, так і асиметричне шифрування даних. Також на його основі можливе підписання даних, що відправляються, електронним цифровим підписом (ЕЦП), що забезпечує цілісність інформації. Відповідно, в базі даних користувачів, з якої здійснює роботу серверна частина ПЗ, містяться другї пари закритих ключів, зашитих у програмах, переданих користувачам системи.

Для захисту інформації від копіювання або прочитання слід застосовувати криптографічні (шифрування) або стеганографічні (приховування факту передачі інформації) методи закриття даних, що передаються.

Можливо також підписання переданих даних ЕЦП, що дозволяє перевірити їх достовірність та цілісність, ідентифікувати відправника.

Стеганографія забезпечує приховання факту наявності або передачі даних. У разі СДН, стеганографії доцільно застосовувати в якості цифрових водяних знаків (ЦВЗ), які забезпечують захист авторських прав. За ним можна однозначно визначити дату їх використання і авторство документа. Крім того, ЦВЗ володіють чудовою властивістю: при зміні вихідного файлу з ЦВЗ самі цифрові знаки не змінюються [2].

Якщо користувачам СДН направляти електронні матеріали, захищені ЦВЗ, то в разі неправомірного копіювання або відтворення отриманих матеріалів можна ідентифікувати порушника по ЦВЗ, а також відновити справжнє авторство. Це повинно стати стримуючим чинником для різного роду зловмисників.

Таким чином, ефективне протистояння загрозам і ризикам у СДН сприятиме не тільки ефективному забезпеченню її інформаційної безпеки, але й організації якісного і конкурентоспроможного процесу навчання у вищому навчальному закладі.

ЛІТЕРАТУРА

1. Андреев А. А. Введение в дистанционное обучение / А. А. Андреев. – М., 1997.
2. Теренин А. А. Безопасность систем дистанционного обучения / А. А. Теренин // Защита информации. Инсайд. – 2008. – № 5. – С. 86–91.

О. П. Грунтов,
кандидат технических наук, доцент,
доцент кафедры компьютерной инженерии
факультета компьютерных наук и инновационных технологий,
Международный гуманитарный университет

ПРОБЛЕМЫ РАЗВИТИЯ ЭЛЕМЕНТНОЙ БАЗЫ КОМПЬЮТЕРОВ

Одним из главных факторов достижения высокого быстродействия, а значит, и высокой производительности компьютера является построение их на новейшей элементной базе. Качество элементной базы является показателем технического прогресса. Степень микроминиатюризации, размер кристалла интегральной схемы (ИС), производительность и стоимость технологии напрямую определяются типом литографии. До настоящего времени доминирующей оставалась оптическая литография, т. е. послойные рисунки на фоторезисторе микросхем наносились световым лучом. В настоящее время ведущие компании, производящие микросхемы, реализуют кристаллы с размерами примерно 400–600 мм^2 для процессоров (например, Pentium) и 200–400 мм^2 – для схем памяти. Минимальный топологический размер (толщина линий) при этом составляет 0,25–0,135 мкм. Для сравнения можно привести такой пример. Толщина человеческого волоса составляет примерно 100 мкм. Значит, при таком разрешении на толщине 100 мкм требуется вычерчивать более двухсот линий.

Дальнейшие успехи микроэлектроники связны с использованием электронной (лазерной), ионной и рентгеновской литографией. Это позволяет выйти на размеры 0,13; 0,10 и даже 0,08 мкм.