УДК 004.031.42

**Герасименко Інна Володимирівна**
старший викладач кафедри комп'ютерних наук та інформаційних технологій управління
Черкаський державний технологічний університет, м. Черкаси, Україна
*gerasimenkoinna@mail.ru*

# ТЕХНОЛОГІЇ ЗАХИСТУ ДАНИХ У СИСТЕМІ ПІДТРИМКИ ДИСТАНЦІЙНОГО НАВЧАННЯ

**Анотація.** Дана стаття присвячена питанням захисту даних у системах підтримки дистанційного навчання. Розглянуті різні засоби захисту, такі як апаратні, програмні, захисні перетворення та організаційний захист. Проаналізовано ключові місця, що потребують захисту, і запропоновано можливі варіанти їх захисту, такі як використання капчі під час реєстрації, захист за IP адресою і сервісом захисту від копіювання. Апробація запропонованих засобів захисту проведена на прикладі електронного навчального курсу «Інформаційні технології аналізу систем», що розгорнутий у системі підтримки прийняття рішень на базі Moodle.

**Ключові слова:** система підтримки дистанційного навчання; електронний навчальний курс; захист даних.

## 1. ВСТУП

Розвиток глобальної комп'ютерної мережі Інтернет відкрив нові перспективи еволюційного вдосконалення світової освітньої системи. Нині традиційні методи освіти доповнюються новими методами навчання, заснованими на використанні Інтернету, комп'ютерних мереж, телекомунікаційних засобів та хмарних сервісів.

Останнім часом навчальні заклади різних країн світу звернули увагу на можливості використання ІКТ для організації дистанційного навчання. Навчання на відстані здавна привертало увагу як педагогів, так і студентів. Таке навчання може набувати різних форм залежно від організації і використовуваних технологій дистанційного навчання (ТДН). До недавнього часу в нашій країні подібне навчання в основному зводилося до обміну друкованою кореспонденцією, епізодичними зустрічами студентів з викладачами під час залікових й екзаменаційних сесій. Це так зване заочне навчання, яке було широко поширене в усіх вищих навчальних закладах країни. В інших країнах для цих цілей широко використовувалися поряд із друкованими засобами можливості телебачення, відеозапису.

Телекомунікаційні системи і мультимедія знайшли застосування практично в усіх сферах життєдіяльності людини. Але, як і будь-який інший предмет, що нас оточує, технології можна використовувати як на благо, так і на шкоду. Завжди є категорія людей, які мають корисливі інтереси, і готових для їх досягнення піти на все, не рахуючись ні з інтересами інших, ні із законами. Так, останнім часом багато проблем розробникам програмного забезпечення докучає незаконне копіювання і розповсюдження програм (так зване програмне піратство). Не є винятком і програмні засоби навчального призначення, а постійні спроби злому хакерами різних систем змушують створювати все більш і більш потужні засоби захисту.

Природно, що проблеми, пов'язані із захистом даних, багатогранні. Й у своїй статті торкнемося і спробуємо розв'язати тільки невелику їх частину, вибравши як напрямки своєї роботи захист даних у системі підтримки дистанційного навчання (СПДН) ВНЗ.

**Постановка проблеми.** СПДН знаходять все більше застосування в навчальному процесі ВНЗ України. Дані системи працюють у режимі монопольного доступу. Під монопольним доступом розуміється можливість користувача здійснювати з програмою будь-які дії, без можливості контролю збоку. Під час розробки таких систем особливу увагу слід приділяти захисту даних від несанкціонованого копіювання, від модифікації програмного коду в інтересах користувача, приховування від користувача частини даних, збереження паролів, захист від перевантажень, а також низки організаційних і технічних питань з провайдером.

На нашу думку, система захисту даних у СПДН має бути багаторівневою і довершеною. Для забезпечення технічного захисту даних потрібно створити комплекс технічного захисту інформації, що є складовою СПДН.

**Аналіз останніх досліджень і публікацій.** Проблема несанкціонованого використання даних у СПДН є актуальною як для освітньої галузі, так і для будь-якого програмного забезпечення загального призначення. Нині існує багато різноманітних засобів захисту, однак відсутня формалізована, науково обґрунтована методика їх проектування. Питанням захисту даних у СПДН приділяється мало уваги або дослідження є застарілими. Лише невелика кількість дослідників займаються цими питаннями. Ознайомлення з їх роботами надало можливість зробити такі висновки: З. У. Альошин, О. С. Бєлокрилова, Д. А. Жолобов, А. А. Мицель, О. Г. Оганесян, М. Ю. Шевельов відзначають, що для систем, які функціонують поза довірчим середовищем, потрібно звернути увагу на: захист від несанкціонованого копіювання, захист від модифікації програмного коду, приховування від користувача частини інформації та низку інших завдань. О. О. Гайша [1] і А. Н. Карпов [2] у своїх роботах зазначають, що проблеми захисту даних у СПДН є досить широкими, і включають створення надійних методик захисту програмного забезпечення персональних комп'ютерів від несанкціонованого використання, а також створення доступних біометричних систем контролю доступу. Також можна знайти роботи, присвячені питанням захисту авторського права (наприклад, Ю. М. Турко [3]).

На нашу думку, важливою проблемою в галузі організації самостійної роботи є слабка захищеність освітнього програмного забезпечення від «злому» з метою доступу до правильних відповідей комп'ютерних тестів, і підробці результатів контролю [4, 5, 6]. Ця проблема випливає з того, що в основному сучасні контролюючі системи будуються на антропоморфному принципі, суть якого полягає у використанні пам'яті комп'ютера для зберігання еталонних відповідей разом із завданнями. Як правило, вони шифруються, але, як показує практика, їх завжди можна розшифрувати. Ця проблема особливо гостро постала з потребою надання віддаленого доступу до даних, де зовнішній контроль знань здійснюється в основному комп'ютером за відсутності викладача.

Існує також проблема захисту навчального програмного забезпечення від модифікації його коду, з метою зміни алгоритму оцінювання результатів тестування, зміна часу для проходження тестування або іншого коду. Слабка захищеність від «злому» будь-яких антропоморфних контролюючих систем створює труднощі в проведенні контролю в СПДН.

З огляду на вище зазначене, дослідження методів захисту даних у СПДН мають велике практичне значення. **Мета статті** полягає в аналіз методів захисту даних без використання допоміжних апаратних засобів для захисту систем, які функціонують в монопольному режимі.

## 2. МЕТОДИ ДОСЛІДЖЕННЯ

Дослідження проводилось в Черкаському державному технологічному університеті (ЧДТУ), зокрема на факультеті інформаційних технологій і систем (ФІТІС) у рамках викладання дисципліни «Інформаційні технології аналізу систем» для студентів напряму підготовки 6.050101 «Комп'ютерні науки», яка належить до дисциплін вільного вибору навчального закладу. Під час дослідження використовувались такі методи: аналіз теоретичних джерел з проблем захисту даних у СПДН, вивчення й узагальнення досвіду провідних ВНЗ, щодо застосування технологій захисту даних, аналіз, оцінювання.

## 3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Забезпечення інформаційної безпеки СПДН ВНЗ є складним комплексом технічних, юридичних та організаційних проблем. Основою для системного розв'язання завдань щодо забезпечення безпеки даних є аналіз можливих ризиків, політика безпеки і план забезпечення безпеки даних. Аналіз ризиків – перший і необхідний етап у розв'язанні задачі захисту даних, який проводиться з метою виявлення переліку потенційно можливих загроз інтересам ВНЗ, подій і можливого збитку, які можуть виникнути в результаті реалізації таких ризиків.

На основі результатів аналізу ризиків у ЧДТУ розробляється політика безпеки – документ, що містить принципи діяльності СПДН ВНЗ щодо проблем безпеки даних. Політика безпеки містить ранжований перелік загроз, які беруться до уваги, визначає бажаний рівень захищеності, описує організаційні рішення, необхідні для розв'язання завдань безпеки даних. На основі затвердженої політики безпеки розробляється план забезпечення безпеки даних, що містить конкретні організаційні і технічні рішення і плани робіт з їх упровадження і реалізації.

Сучасні засоби захисту від несанкціонованого доступу широко представлені на ринку. В основному вони є програмно-апаратними комплексами із застосуванням особистого ідентифікатора (електронний ідентифікатор сімейства Touch Memory (iButton), мікропроцесорна карта і т. д.). Продукти цього класу надають можливість розмежувати доступ до інформаційних ресурсів обчислювальної техніки, вести аудит сеансів роботи, адмініструвати використовувані програмні засоби. Попри це, деякі з них мають вбудовані антивірусні функції і засоби криптографічного захисту інформації. У разі мережевого використання захисту робочих місць є можливість віддаленого адміністрування кожного з них й отримання повної статистики спроб доступу до комп'ютера і сеансів роботи.

Слід зазначити, що програмним аналізаторам протоколів систем за всієї зручності роботи з ними, властивий суттєвий недолік, пов'язаний з необхідністю використання виділеної робочої станції для виконання завдань з аналізу мережевого трафіку. Це рішення не завжди прийнятне через жорстку прив'язку аналізатора до топології мережі.

Практика показує, що корпоративна мережа ВНЗ є достатньо живим організмом, і важко заздалегідь визначити ту ділянку мережі, яка потребує підвищеного рівня контролю з боку адміністратора безпеки. Необхідність встановлення стаціонарних аналізаторів у конкретних точках корпоративної мережі визначається відповідно з політикою безпеки, прийнятою у ВНЗ.

Захист у СПДН ФІТІС можна розглядати за чотирма напрямками:

- апаратний захист;
- програмний захист;
- захисні перетворення;

– організаційний захист.

Нині гостро стоїть питання про якість знань, отриманих з використанням ТДН. За очної форми навчання більшість викладачів ведуть облік відвідуваності студентів. З переходом на дистанційну освіту аудиторія студентів збільшилася в кілька разів, і враховувати відвідуваність студентів проблематично. Дистанційне навчання висуває певні вимоги до психологічних особливостей студентів. По-перше, у нього повинна бути висока стійка мотивація до отримання освіти. По-друге, студент досить чітко повинен представляти бажаний результат навчання. І, по-третє, він має розуміти, що несе відповідальність за знання, отримані з допомогою СПДН. У багатьох твердження про те, що дистанційне навчання забезпечує студенту вільний графік навчання, асоціюється з вільним відвідуванням сервера СПДН. У зв'язку з цим існує ймовірність підтасувати дані або змінити оцінки та інше.

Розглянемо захист даних у СПДН ФІТІС [7] на прикладі викладання дисципліни «Інформаційні технології аналізу систем» (ІТАС).

СПДН ФІТІС, яка виступає як об'єкт захисту, може моделюватися у вигляді сукупності взаємодіючих вузлів. Вузлами можуть виступати робочі станції користувачів, сервери або комунікаційне обладнання. У даній моделі кожен вузол СПДН представлений трьома рівнями:

1) рівнем апаратного забезпечення. На цьому рівні функціонують технічні засоби вузла, такі як мережеві адаптери, процесори, мікросхеми плат та ін;

2) рівнем загальносистемного програмного забезпечення, на якому функціонує операційна система вузла і всі її складові модулі;

3) рівнем прикладного програмного забезпечення. На цьому рівні функціонує програмне забезпечення, що забезпечує розв'язання прикладних задач, для яких призначена система.

Одним із завдань дослідження була побудова захисту в СПДН при авторизації нових користувачів. Ця проблема розв'язується завдяки ручній реєстрації в СПДН, кожен студент отримує своє вхідне ім'я і пароль для входу до систему.

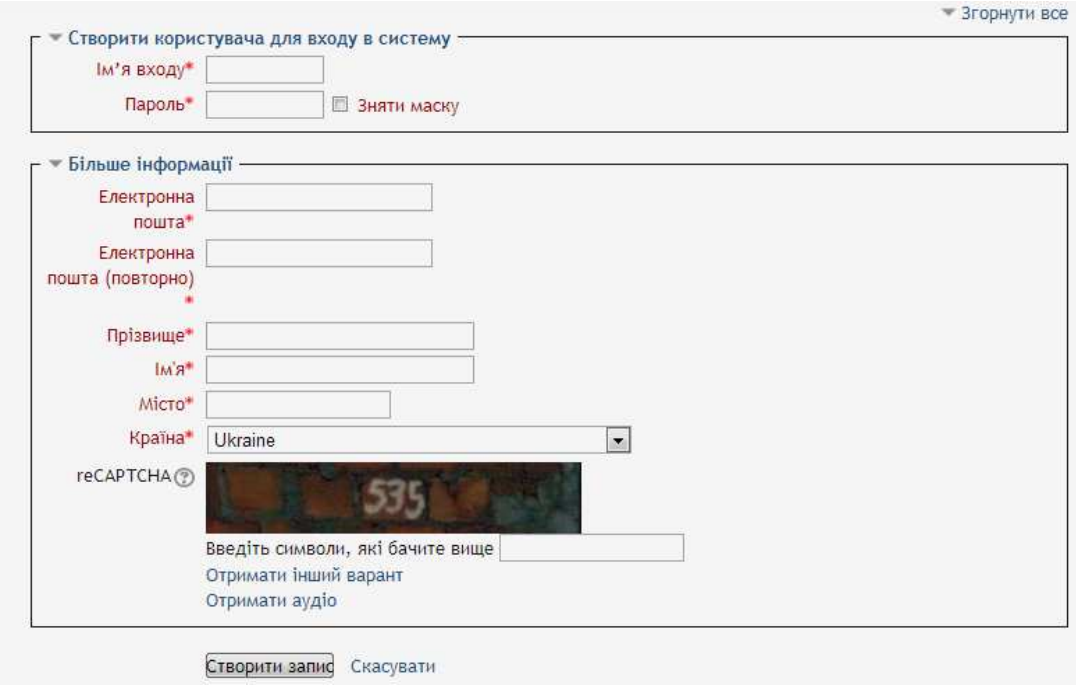


*Рис. 1. Вікно реєстрації в СПДН ЧДТУ*

У рамках написання роботи було виконано низку вдосконалень на різних рівнях, зокрема до вікна реєстрації нового користувача додано «капчу» (рис. 1). Після реєстрації студент отримує доступ до системи.

Одним з основних елементів політики безпеки в СПДН є довільне керування доступом. Довільне керування доступом – це метод обмеження доступу до об'єктів, заснований на обліку особистості суб'єкта або групи, у яку суб'єкт входить. Довільність управління полягає в тому, що адміністратор СПДН може надавати студентам або відбирати у них права доступу до системи й електронного навчального курсу ЕНК. Також адміністратор системи має можливість розмежування прав доступу (рис. 2): гість; студент; асистент; викладач; автор курсу; секретар деканату і т. д.

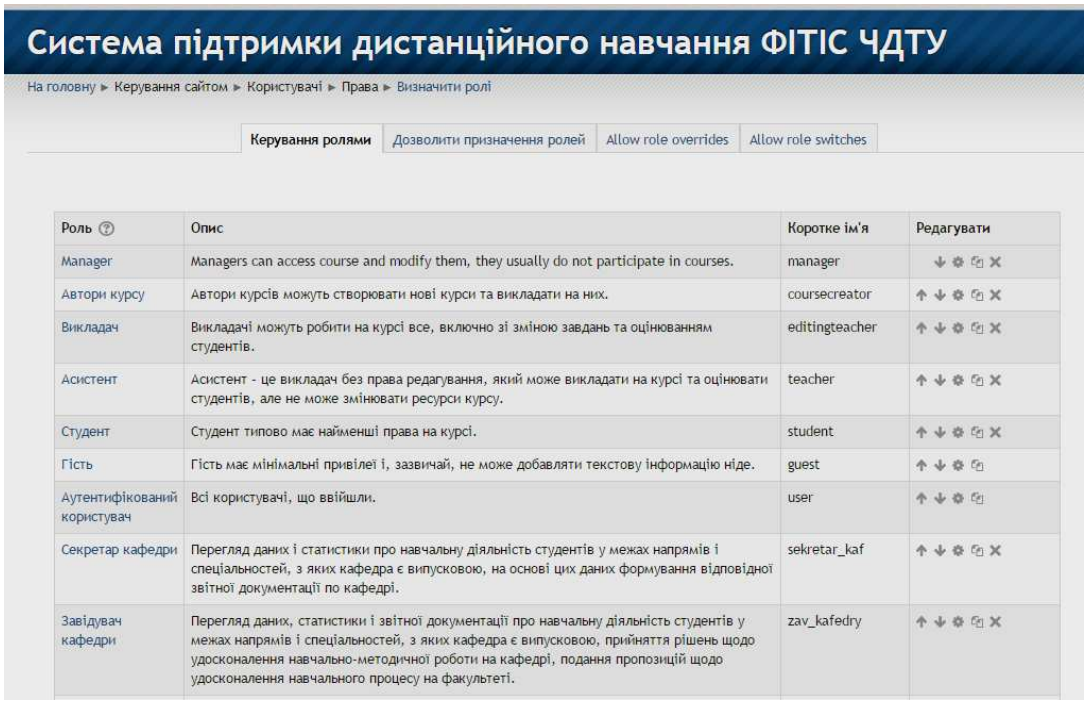


*Рис. 2. Вікно адміністрування прав користувачів*

Надати відповідні права в ЕНК може і сам викладач курсу (рис. 3).

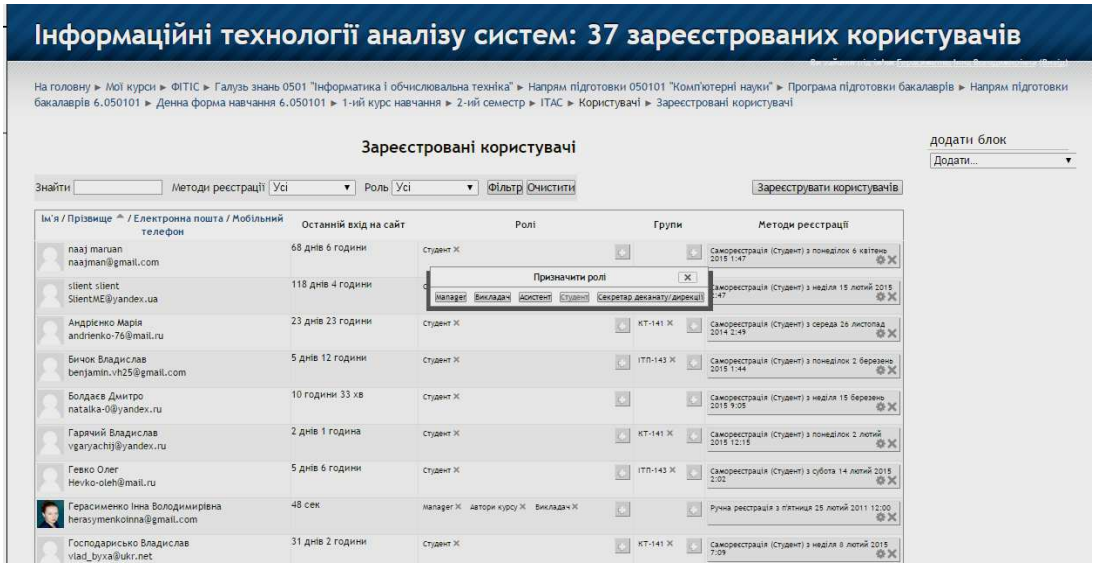


*Рис. 3. Вікно призначення ролей в ЕНК*

За необхідності адміністратор сервера, на якому розгорнуто СПДН, може за допомогою інформації, що збирається, відновити будь-який сценарій сеансу роботи будь-якого студента чи зареєстрованого користувача, а саме:

- перелік сторінок, відвіданих студентом за сеанс роботи;
- час, проведений на кожній сторінці;
- активовані гіперпосилання на даній сторінці;
- перелік файлів, які були скопійовані студентом з навчального сервера;
- час тестування та ін.

Але вся так зібрана інформація є непрямою. Тобто, якщо в систему увійшов студент з використанням логіна і пароля свого колеги з метою відзначитися і взяти участь у тестуванні, то його неможливо викрити. Іншими словами, потрібні прямі докази того, що даний сеанс навчання провів справді той студент, з чиїм ім'ям зіставлені вхідне ім'я і пароль. Існує ймовірність того, що для тестування студент може посадити за комп'ютер замість себе більш обізнану в предметі людину. Навігаційна система СПДН має перевіряти, чи знаходиться за віддаленим комп'ютером саме той, кого навчають, тобто, зробити розпізнавання користувача.

У рамках даної роботи також було розв'язано проблему ідентифікації користувача і захисту даних під час комп'ютерного тестування засобами СПДН. У разі використання даної системи в комп'ютерних лабораторіях, ніяких складнощів не виникає, оскільки студенти перебувають під контролем викладача. Але орієнтація освіти на дистанційне навчання вносить свої корективи. Виникає потреба в можливості використання даного програмного забезпечення студентом на своїй локальній машині. Для убезпечення від несанкціонованого доступу до тестових завдань, що розміщені в СПДН ФІТІС було додано форму для підтвердження реальності користувача (перевірка sms сервісом). Принцип роботи досить простий. Під час входження до тесту студенту потрібно заповнити форму підтвердження реальності користувача (рис. 4). Після чого на мобільний телефон прийде код для підтвердження авторизації (рис. 5). Далі потрібно ввести отриманий код (рис. 6), після чого система вітає користувача з успішним підтвердженням авторизації (рис. 7).

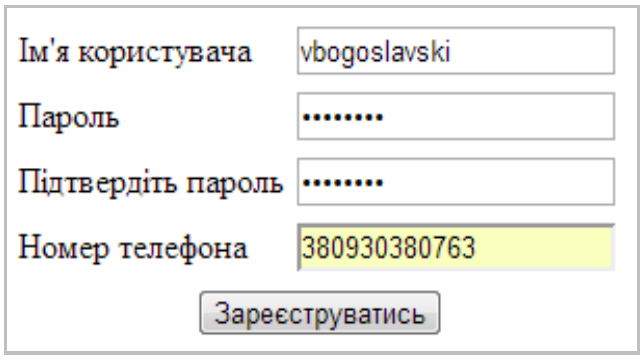


*Рис. 4. Форма підтвердження реальності користувача*


*Рис. 5. Sms повідомлення з кодом підтвердження*

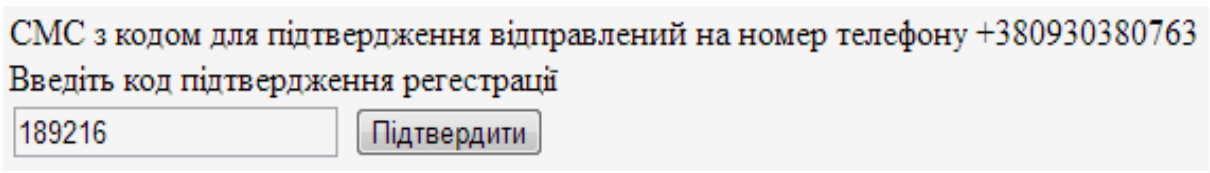


*Рис. 6. Вікно введення коду для підтвердження користувача*

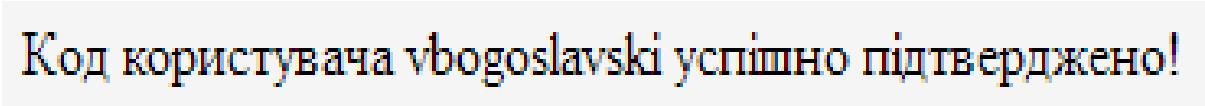


*Рис. 7. Вікно підтвердження користувача*

Іншим варіантом убезпечення доступу до комп'ютерного тестування є робота системи з використанням захисту за IP на рівні входження в систему, тобто доступ до системи здійснюється лише з комп'ютерної лабораторії університету (рис. 8).

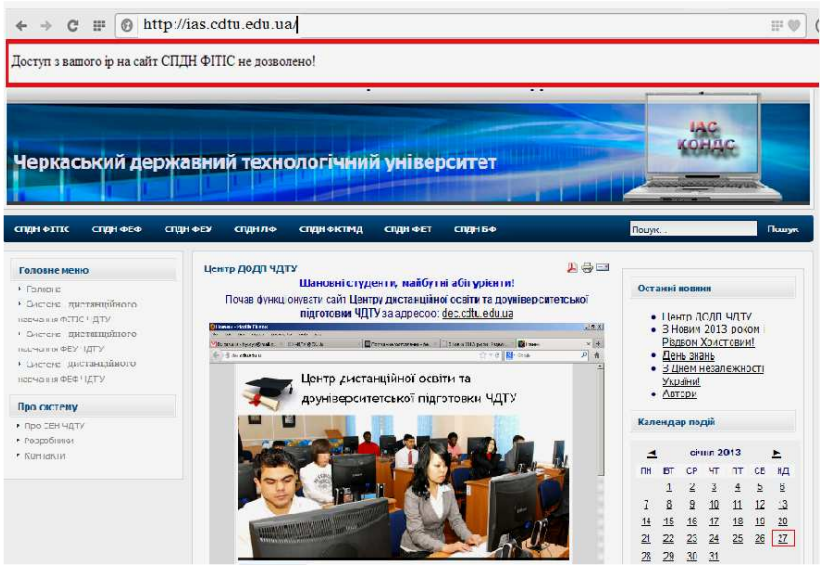


*Рис. 8. Приклад роботи системи захисту за IP адресою на рівні входження в систему*

Ще один варіант захисту під час проходження комп'ютерного тестування засобами СПДН – це робота сервісу захисту від копіювання (рис. 9). Даний сервіс досить легко налаштовується засобами тестування в самій системі.

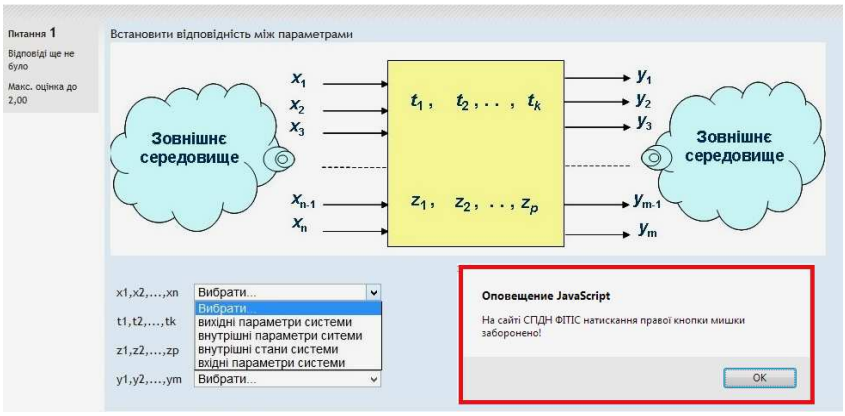


*Рис. 9. Приклад роботи сервісу захисту від копіювання інформації*

Для захисту особистих файлів у СПДН ФІТІС використовується протокол HTTTPS (рис. 10).

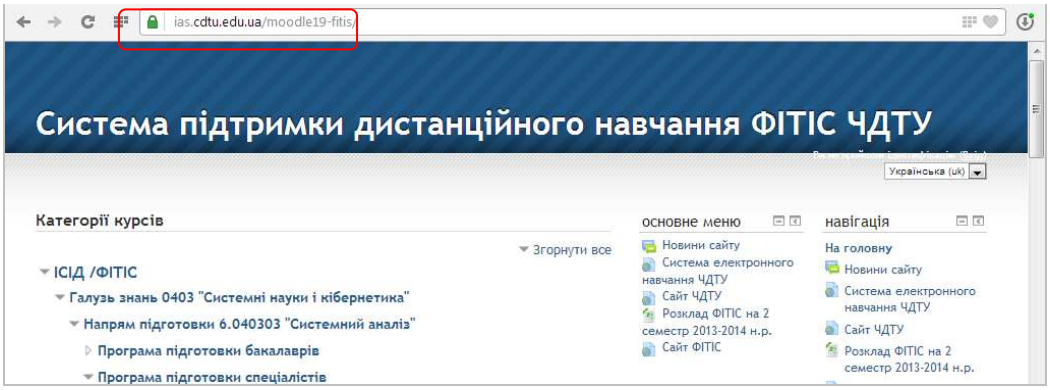


*Рис. 10. Приклад роботи СПДН ФІТІС через протокол HTTPS*

Отже, нами було розглянуто основні напрями роботи із захисту СПДН.

## 4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

З вище викладеного випливає, що проблема захисту даних у СПДН дійсно актуальною і вимагає до себе уваги. наразі, на даний момент напрацювань у цій галузі досить мало. Велика частина системи захисту лежить поза сферою можливості програмного забезпечення і вимагає відповідної адміністративної організації і контролю, що говорить про необхідність розробки теоретичних і практичних методик розробки СПДН й ЕНК із застосуванням систем захисту даних. Цей розділ, можливо, можна віднести до педагогічних наук. Але сама собою педагогіка не здатна, без технічної підтримки побудувати таку СПДН, яка б відповідала всім вимогам, як з боку якості навчання, так і з точки зору організації контролю в такому навчанні. Отже, рішення для організації навчання з допомогою СПДН може дати тільки симбіоз педагогічних і технічних наук. А, отже, основним завданням інформаційних технологій є побудова необхідної технічної бази для подальшого їх використання в СПДН ВНЗ.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гейша О. О. Методики забезпечення захищеності систем дистанційної освіти : дис. ... канд. тех. наук: 05.13.06 / Олександр Олександрович Гайша. – К., 2008. – 165 с.
2. Карпов А. Н. Защита информации в системах дистанционного обучения с монопольным доступом : автореф. ... магистр техники и технологий : 553000 / А. Н. Карпов. – Тула, 2014. – 21 с.
3. Турко Ю. М. Проблеми захисту авторського права в системах дистанційної освіти / Ю. М. Туркот, О. С. Ворокін // Всеукраїнський конкурс студентських наукових робіт з природничих, технічних та гуманітарних наук у 2011/2012 навчальному роках. [Електронний ресурс]. – Режим доступу : http://tdo.at.ua/voronkin/konkurs.pdf.
4. Махутов Б. Н. Защита электронных учебников в дистанционном обучении / Махутов Б. Н., Шевелев М. Ю. // Образование XXI века: инновационные технологии, диагностика и управление в условиях информатизации и гуманизации : м атериалы III Всероссийской научно-методической конференции с международным участием. – Красноярськ : КГПУ, 2001. – С. 106–108.
5. Шелупанов А. А. Анализ проблемы информации в системе дистанционного образования / Шелупанов А. А., Пряхин А. В. // Современное образование: массовость и качество. Тез. докл. региональной научно-методической конференции. – Томск : ТУ СУР, 2001. – С. 159–161.
6. Кацман Ю. Я. Применение компьютерных технологий при дистанционном обучении студентов // Тез. докладов региональной научно методической конференции «Современное образование: массовость и качество». – Томск : ТУСУР, 2011. – С. 170–171.

7. Система підтримки дистанційного навчання Факультету інформаційних технологій і систем [Електронний ресурс]. – Режим доступу : http://ias.cdtu.edu.ua/moodle19-fitis/.

*Матеріал надійшов до редакції 25.04.2015 р.*

# ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ В СИСТЕМЕ ПОДДЕРЖКИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

**Герасименко Инна Владимировна**
старший преподаватель кафедры компьютерных наук и информационных технологий управления
Черкасский государственный технологический университет, г. Черкассы, Украина
*gerasimenkoinna@mail.ru*

**Аннотация.** Данная статья посвящена вопросам защиты данных в системах поддержки дистанционного обучения. Рассмотрены различные средства защиты, такие как аппаратные, программные, защитные преобразования и организационная защита. Проанализированы ключевые места, требующие защиты и предложены возможные варианты их защиты, такие как использование капчи при регистрации, защита по IP-адресу и сервису защиты от копирования. Апробация предложенных средств защиты проведена на примере электронного учебного курса «Информационные технологии анализа систем», который изложен в системе поддержки принятия решений на базе Moodle.

**Ключевые слова:** система поддержки дистанционного обучения; электронный учебный курс; защита данных.

# DATA PROTECTION TECHNOLOGIES IN THE DISTANCE LEARNING SYSTEMS

**Inna V. Herasymenko**
senior lecturer, Department of Computer Sciences and Information Technologies Management
Cherkasy State Technological University, Cherkasy, Ukraine
*gerasimenkoinna@mail.ru*

**Abstract.** This article focuses on data protection in the support systems of distance learning. Different security tools such as hardware, software, transformation security and organizational protection are considered. There are analyzed key places that require protection and suggested possible options for their protection, such as the use of CAPTCHA for registration, protection for the IP-address and service of copy protection. Testing of the proposed security tools was piloted in terms of e-learning course "Information Technologies of Systems Analysis".

**Keywords:** support system of distance learning; electronic learning course; data protection.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Geisha O. O. Methods to ensure the integrity of distance education, Thesis ... candidate. those. Sciences : 05.13.06 / Alexander Haysha. – K., 2008. – 165 p. (in Russian).
2. Karpov A. N. Security of information systems with learning monopolnm remote access: Abstract. ... Master of Technics and Technology : 553 000 / A. N. Karpov. – Tula, 2014. – 21 p. (in Russian).
3. Turco Y. M. Problems of copyright in systems of distance education [online] / Y. M. Turkot, O. S. Vorokin // Ukrainian competition of student research papers on natural, technical and humanities in 2011/2012 academic years. – Available from : http://tdo.at.ua/voronkin/konkurs.pdf (in Ukrainian)/.
4. Mahutov B. N. Security of electronic textbooks in Distance leasrining / Mahmutov B. N, Shevelev M. U. // Education XXI century: Innovaczionnye technologies, diagnostics and Local Government in terms ynformatyzatsyy and humanyzatsyy: Materials III Vserossyyskoy metodycheskoy

scientific conference with participation mezhdunarodnm. – Krasnoyarsk : KHPU, 2001. – S. 106–108 (in Russian).
5. Shelupanov A. A. Analysis of the problems of information in the system of distance education / A. A. Shelupanov A. V. Pryakhin // Modern Education: massovost and quality. Tez. Dokl. rehyonalnoy metodycheskoy scientific conference. – Tomsk : TU AUR, 2001. – S. 159–161 (in Russian).
6. Katzman U. Y. Application of computer technology in the students distance learning // Proc. dokladov rehyonalnoy metodycheskoy scientific conference «Modern Education: massovost and Quality». – Tomsk : TUSUR, 2011. – P. 170–171 (in Russian).
7. The system of distance learning Faculty of Information Technologies and Systems [online]. – Available from: http://ias.cdtu.edu.ua/moodle19-fitis (in Ukrainian).