legal support to stimulate their implementation mechanisms, as well as during the active infrastructure development of innovative processes in educational activities. This should contribute to the concentration of efforts on the priority directions of development of information and innovative technologies used in educational institutions.

References

1. Bykov V. Yu. Innovative development of society and modern network technology of open education // Collection of scientific papers. Department of "Pedagogy and Psychology of social systems" National Technical University "HPI" "Problems and prospects of forming national humanitarian and technical elite". – 2010. – Vol. 28. – P. 25–50. 2. Research universities Ukraine, available at: http://osvita.ua/vnz/glossary/3868/ 3. Yevstigneyeva L., Yevstigneyev R. The mystery of the catching-up // Voprosy ekonomiki. – 2013. – Vol. 1. – P. 81–96. 4. Basic indicators of higher educational institutions of Ukraine at the beginning of 2015/16 school year. Statistical bulletin / K. State Statistics Service of Ukraine. – 2016.є – P. 171. 5. Safonova V. Ye. Higher education – resource formation of innovative economy Monograph // K. AgrarMediaGrup Ltd. – 2011. – P. 336. 6. Yakovenko L. I., Pashchenko O. V. The economic fundamentals of the modernization of higher education in becoming a knowledge economy // Poltava pub. Skytek. – 2011. – P. 216. 7. Botlin I. W., Elmandjra M., Malitza M. No Limits to Learning. A. Report to the Club of Rome Oxford etc., 1979. – P. 25–30. 8. Franki V. Man in search of sense: Collection / Per. Sangl i nem. D. A. Leontieva, M. P. Papusha, E. V. Jejdmana. – M.: Progress, 1990. – 368 p.

УДК 004.031.42

Інна Герасименко
Черкаський державний технологічний університет

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ДИСТАНЦІЙНОГО НАВЧАННЯ

Розглянуто питання захисту даних у системах підтримки дистанційного навчання, різні засоби захисту, такі як апаратні, програмні, захисні перетворення та організаційний захист. Проаналізовано ключові місця, що потребують захисту, та запропоновано можливі варіанти їх захисту, такі як використання капчі під час реєстрації, захист за IP-адресою та сервісом захисту від копіювання. Апробацію запропонованих засобів захисту проведено на прикладі електронного навчального курсу "Інформаційні технології аналізу систем", розгорнутого в системі підтримки прийняття рішень на базі Moodle.

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

This article is devoted to the protection of data systems in support of distance learning. Describes various remedies, such as hardware, software, protective transformations, and organizational protection. The key areas that need protection and suggested possible options for their protection, such as a captcha in the registration, protection class IP address and service of the copy protection are analyzed. The proposed remedies undertaken on the example of e-learning course "Information technology analysis, systems" deployed in the system of decision support based on Moodle.

Key words: system in support of distance learning; e-learning course; data protection.

Вступ

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

Останніми роками 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). Донедавна в нашій країні таке навчання зводилося переважно до обміну друкованою кореспонденцією, епізодичних зустрічей студентів з викладачами під час залікових та екзаменаційних сесій. Це так зване заочне навчання, яке було дуже поширене в усіх вищих навчальних закладах країни. В інших країнах для цих цілей широко використовувалися поряд з друкованими засобами можливості телебачення, відеозапису.

Телекомунікаційні системи та мультимедіа застосовують практично у всіх 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 з корисливими інтересами, які готові для їх досягнення піти на все, не рахуючись ні з інтересами інших, ні із законами. Так, останнім часом багато проблем розробникам програмного забезпечення створює незаконне копіювання та розповсюдження програм (так зване програмне піратство). Не є винятком і програмні засоби навчального призначення, а постійні спроби хакерів зламати різні системи змушують створювати все потужніші засоби захисту.

Природно, що проблеми, пов'язані із захистом даних, багатогранні. І в своїй статті я хочу торкнутися і спробувати вирішити тільки невелику їх частину, вибравши як напрями своєї роботи захист даних у системі підтримки дистанційного навчання (СПДН) ВНЗ.

Постановка проблеми

СПДН все ширше застосовують у навчальному процесі ВНЗ України. Ці системи працюють у режимі монопольного доступу. Під монопольним доступом розуміють можливість користувача здійснювати з програмою будь-які дії, без можливості контролю з боку. Розробляючи такі системи, особливу увагу треба приділяти захисту даних від несанкціонованого копіювання, від модифікації програмного коду в інтересах користувача, приховуванню від користувача частини даних, збереженню паролів, захисту від перевантажень, а також низці організаційних і технічних питань з провайдером.

На нашу думку, система захисту даних у СПДН має бути багаторівневою та 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 актуальна 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 приділяють недостатньо уваги або дослідження є застарілими, лише декілька дослідників займаються цими питаннями. Ознайомлення з їхніми роботами надало можливість зробити такі висновки: З. У. Альошин, О. С. Бєлокрилова, Д. А. Жолобов, А. А. Мицель, О. Г. Оганесян, М. Ю. Шевельов зазначають, що для систем, що 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] та А. Н. Карпов [2] у своїх роботах зазначають, що проблеми захисту даних у СПДН доволі широкі й охоплюють створення надійних методик захисту програмного забезпечення персональних комп'ютерів від несанкціонованого використання, а також доступних біометричних систем контролю доступу. Також можна знайти роботи з питань захисту авторського права (наприклад, Ю. М. Турко [3]).

На нашу думку, важливою проблемою у сфері організації самостійної роботи є слабка захищеність освітнього програмного забезпечення від "злому" з метою доступу до правильних відповідей комп'ютерних тестів і підроблення результатів контролю [4–6]. Ця проблема випливає з того, що переважно сучасні системи контролю будуються на антропоморфному принципі, суть якого полягає у використанні пам'яті комп'ютера для зберігання еталонних відповідей разом із

завданнями. Як правило, їх шифрують, але, як показує практика, завжди можна розшифрувати. Ця проблема особливо загострилась з потребою надання віддаленого доступу до даних, коли зовнішній контроль знань здійснює переважно комп'ютер за відсутності викладача.

Існує також проблема захисту навчального програмного забезпечення від модифікації його коду, з метою зміни алгоритму оцінювання результатів тестування, зміни часу для проходження тестування або іншого коду. Слабка захищеність від "злому" будь-яких антропоморфних систем контролю створює труднощі під час проведення контролю у СПДН.

З огляду на зазначене вище, дослідження методів захисту даних у СПДН має велике практичне значення.

Мета статті полягає в аналізі методів захисту даних без використання допоміжних апаратних засобів для захисту систем, які функціонують у монопольному режимі.

Виклад основного матеріалу

Забезпечення інформаційної безпеки СПДН ВНЗ являє собою складний комплекс технічних, юридичних та організаційних проблем. Основою для системного вирішення завдань щодо забезпечення безпеки даних є аналіз можливих ризиків, політика безпеки та 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 можливих збитків, які можуть виникнути в результаті реалізації таких ризиків.

На основі результатів аналізу ризиків в ЧДТУ розробляється політика безпеки – документ, що містить принципи діяльності СПДН ВНЗ щодо проблем безпеки даних. Політика безпеки містить ранжований перелік загроз, які треба враховувати, визначає бажаний рівень захищеності, описує організаційні рішення, необхідні для вирішення завдань безпеки даних. На основі затвердженої політики безпеки розробляється план забезпечення безпеки даних, що містить конкретні організаційні та технічні рішення і плани робіт з їх впровадження та реалізації.

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

Зазначимо, що програмні аналізатори протоколів систем, за всієї зручності роботи з ними, мають істотний 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 – доволі живий організм, 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 до політики безпеки, прийнятої у ВНЗ.

Захист у СПДН ФІТІС можна розглядати за чотирма напрямами:

- апаратний захист;
- програмний захист;
- захисні перетворення;
- організаційний захист.

Сьогодні гостро стоїть питання про якість знань, отриманих з використанням ТДН [7]. 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 ставить певні вимоги до психологічних особливостей студентів. По-перше, у нього повинна бути висока стійка мотивація до отримання освіти. По-друге, студент доволі чітко повинен уявляти бажаний результат навчання. І, по-третє, він повинен розуміти, що відповідає за знання, отримані за допомогою СПДН. У багатьох твердження про те, що дистанційне

навчання забезпечує студентові вільний графік навчання, асоціюється з вільним відвідуванням сервера СПДН. Тому існує ймовірність підтасування даних або змін оцінок тощо.

Розглянемо захист даних у СПДН ФІТІС [8] на прикладі викладання дисципліни "Інформаційні технології аналізу систем" (ІТАС).

СПДН ФІТІС, яка виступає об'єктом захисту, може моделюватися у вигляді сукупності вузлів, що взаємодіють. Вузлами можуть бути робочі станції користувачів, сервери або комунікаційне обладнання. У цій 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 тощо;

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 вирішення прикладних завдань, для яких призначена система.

Одним із завдань дослідження була побудова захисту в СПДН під час авторизації нових користувачів. Ця проблема вирішується завдяки ручній реєстрації в СПДН, кожен студент отримує своє вхідне ім'я та пароль для входу до систему. Під час написання роботи було здійснено низку вдосконалень на різних рівнях, зокрема до вікна реєстрації нового користувача додано "капчу" (рис. 1). Після реєстрації студент отримує доступ до системи.

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

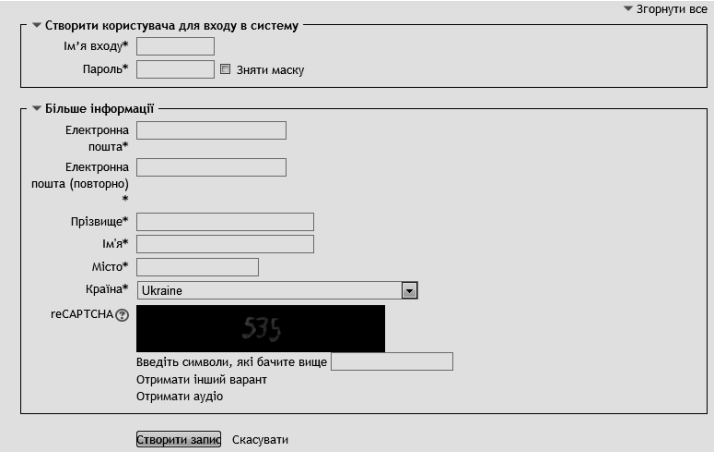

Рис. 1. Вікно реєстрації у СПДН ЧДТУ

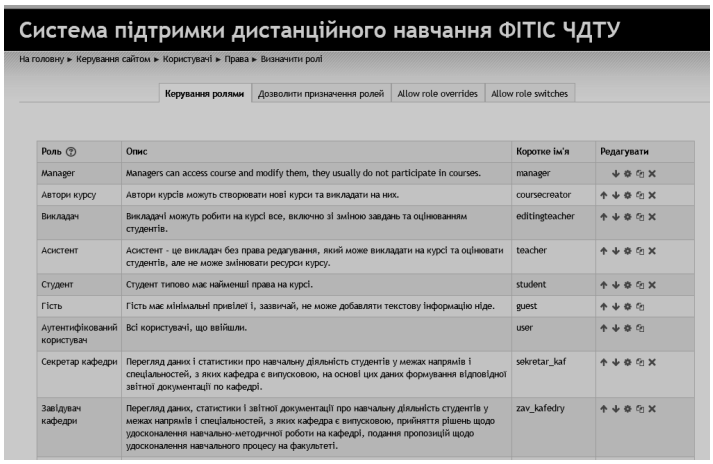

Рис. 2. Вікно адміністрування прав користувачів

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, які відвідав студент за сеанс роботи;

– час, проведений на кожній сторінці;

– активовані гіперпосилання на цій сторінці;

– перелік файлів, які скопіював студент з навчального сервера;

– час тестування тощо.

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

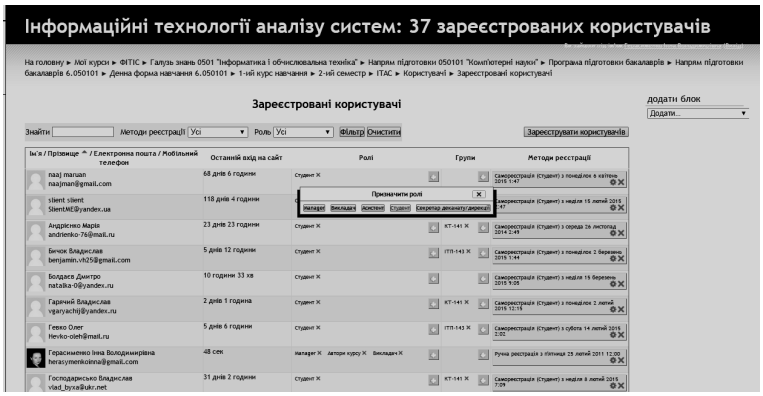

Рис. 3. Вікно призначення ролей в ЕНК

Але вся зібрана у такий спосіб інформація є непрямою. Тобто якщо в систему увійшов студент з використанням логіна та пароля свого колеги, щоб відзначитися і взяти участь у тестуванні, то його неможливо викрити. Інакше кажучи, потрібні прямі докази того, що цей сеанс навчання провів справді той студент, з чиїм ім'ям зіставлені вхідне ім'я і пароль. Існує ймовірність того, що під час тестування студент може посадити за комп'ютер замість себе обізнанішу у предметі людину. Навігаційна система СПДН повинна перевіряти, чи за віддаленим комп'ютером перебуває саме той, кого навчають, тобто здійснити розпізнавання користувача.

У межах цієї роботи також було вирішено проблему ідентифікації користувача та захисту даних під час комп'ютерного тестування засобами СПДН. У разі використання цієї 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 цього програмного забезпечення студентом на своїй локальній машині. Для убезпечення від несанкціонованого доступу до тестових завдань, що розміщені в СПДН ФІТІС, додано форму для підтвердження реальності користувача (перевірка sms-сервісом). Принцип роботи доволі простий. Входячи до тесту, студент повинен заповнити форму підтвердження реальності користувача (рис. 4). Після цього на мобільний телефон надійде код для підтвердження авторизації (рис. 5). Далі потрібно ввести отриманий код (рис. 6), після чого система вітає користувача з успішним підтвердженням авторизації (рис. 7).

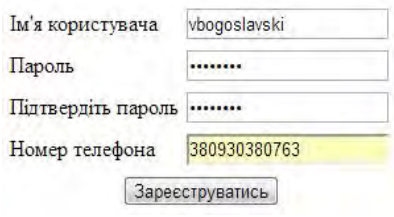

Рис. 4. Форма підтвердження реальності користувача

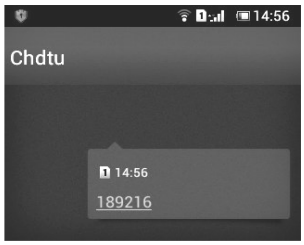

Рис. 5. Sms повідомлення з кодом підтвердження

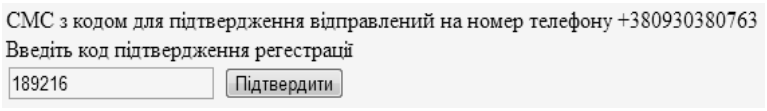

Рис. 6. Вікно введення коду для підтвердження користувача

Рис. 7. Вікно підтвердження користувача

Іншим варіантом убезпечення доступу до комп'ютерного тестування є робота системи з використанням захисту за IP на рівні входження у 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 у систему

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

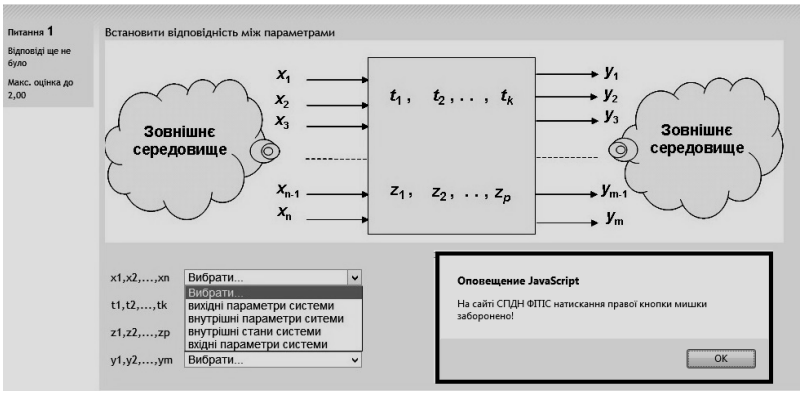

Рис. 9. Приклад роботи сервісу захисту від копіювання інформації

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

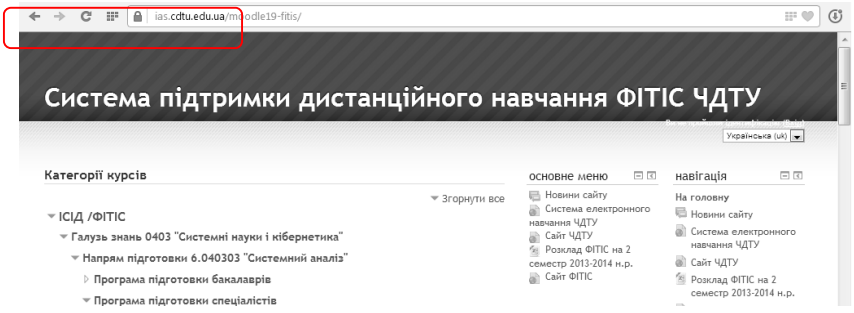

Рис. 10. Приклад роботи СПДН ФІТІС через протокол HTTPS

Так було розглянуто основні напрями роботи із захисту СПДН.

Висновки та перспективи подальших досліджень

З викладеного вище випливає, що проблема захисту даних у СПДН справді актуальна і потребує уваги. Однак поки що напрацювань у цій галузі доволі мало. Велика частина системи захисту – поза сферою можливості програмного забезпечення і потребує відповідної адміністративної організації та контролю, що свідчить про необхідність створення теоретичних і практичних методик розроблення СПДН та ЕНК з застосуванням систем захисту даних. Цей розділ, мабуть, можна зарахувати до педагогічних наук. Але сама по собі педагогіка не здатна без технічної підтримки побудувати таку СПДН, яка б відповідала всім вимогам, і з боку якості навчання, і з погляду організації контролю за такого навчання. Отже, рішення для організації навчання за 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 у СПДН ВНЗ.

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 ситтемах 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: материалы III Всерос. научно-метод. конф. с междунар. участием. – Красноярск: 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. регион. науч.-метод. конференции. – Томск: ТУ СУР, 2001. – С. 159–161. 6. Кацман Ю. Я. Применение компьютерных технологий при дистанционном обучении студентов // тез. докладов регион. научн.-метод. конференции "Современное образование: массовость и качество". – Томск: ТУСУР, 2011. – С. 170–171. 7. Герасименко І. В. Методика використання технологій дистанційного навчання в підготовці бакалаврів комп'ютерних наук: дис. … канд. пед. наук: 13.00.10 / Інна Володимирівна Герасименко – К., 2015. – 302 с. 8. Система підтримки дистанційного навчання Факультету інформаційних технологій і систем [Електронний ресурс]. – Режим доступу:* http://ias.cdtu.edu.ua/moodle19-fitis/

Inna Herasymenko
Cherkasy State Technological University

USED DISTANCE LEARNING TECHNOLOGIES

Introduction

The development of a global computer network Internet has opened new prospects for an evolutionary improvement of world educational system. Today traditional education methods are supplemented with new teaching methods based on the use of the Internet, computer networks, telecommunications, cloud services and distance learning technologies.

Analysis of the latest sources of literature

The problem of unauthorized use of data in system of distance learning is relevant for the educational sector, and for any general purpose software. Today there are many different remedies, but

there is no formalized, scientifically proven method of their design. The issue of data protection in system of distance learning paid little attention or investigation is outdated. Only a small number of researchers involved in these issues: S. V. Aleshin, O. S. Byelokrylova, D. A. Zholobov A. A. Mytsel, O. G. Hovhannisyan, M. Y. Shevelev, A. A. Haysha and A. N. Karpov.

Purpose of the research

This article is devoted to the protection of data systems in support of distance learning. Describes various remedies, such as hardware, software, protective transformations, and organizational protection. The key areas that need protection and suggested possible options for their protection, such as a captcha in the registration, protection class IP address and service of the copy protection are analyzed.

Discussion

Modern means of protection from unauthorized access widely available on the market. Basically they are a hardware-software systems using personal identification, microprocessor card. Practice shows that the corporate network university is a very living organism, and it is difficult to determine in advance that area network that requires a high level of control by the security administrator. The need to establish stationary analyzers to specific points of the corporate network is determined in accordance with the security policy adopted in universities.

Conclusions

It follows from the above that the problem of data protection in system of distance learning really urgent and requires attention. Thus, at the moment of developments in this area very few. Most of the protection system is beyond the scope and possibilities of the software requires an appropriate administrative organization and control. That suggests the need to develop theoretical and practical methods system of distance learning development and application of and e-learning course of data protection. This section probably can be attributed to educational sciences. But education by itself is not capable, without technical support to build such SPDN that would meet all the requirements of both the quality of education, and from the perspective of control in this study. Thus, the solution for learning through system of distance learning can only give symbiosis pedagogical and technical sciences. And, therefore, the main task is to build information technology necessary technical framework, for later use in SPDN universities.

References

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 of 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 syttemah distance education / Y. M. Turkot, O. S. Vorokin // Ukrainian competition of student research papers on natural, technical and humanities in 2011/2012 academic years [Electronic resource]. – Access: http://tdo.at.ua/voronkin/konkurs.pdf. (in Ukrainian). 4. Mahutov B. N. Security e`lektronny'h in uchebnykov of Remote Learning / 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 Remote 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 learning of Remote studentov // Proc. dokladov rehyonalnoy metodycheskoy scientific conference "Modern Education: massovost and Quality". – Tomsk: TUSUR, 2011. – P. 170–171. (in Russian). 7. Gerasimenko I. V. System elearning future professionals in higher technical educational institutions: dis. … PhD of Philosophy: 13.00.10 / Inna Gerasimenko. – K., 2015. – 302 c. 8. The system of distance learning Faculty of Information Technologies and Systems [Electronic resource]. – Access: http://ias.cdtu.edu.ua/moodle19-fitis. (in Ukrainian).