НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
Радіотехнічний факультет
(повна назва інституту/факультету)

Кафедра теоретичних основ радіотехніки
(повна назва кафедри)

«На правах рукопису»
УДК __004.7_____

«До захисту допущено»
Завідувач кафедри
_____ Ф.Ф. Дубровка
(підпис) (ініціали, прізвище)
“___”_____2015 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності ___8.05090103 Радіоелектронні пристрої, системи та комплекси___
(код і назва)

на тему: Розробка структури та програмного забезпечення універсальної галузевої інтерактивної мережі з можливістю шифрування персональних даних

Виконав (-ла): студент (-ка) _6_ курсу, групи _РС-31м__
(шифр групи)

_____Товкач Ігор Олегович_____ _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник __доцент, к.т.н., с.н.с. Піддубний В.О._____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант охорона праці ___к.т.н., доцент Каштанов С.Ф. __ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2015 року

Національний технічний університет України
«Київський політехнічний інститут»

Інститут (факультет) Радіотехнічний факультет
(повна назва)

Кафедра теоретичних основ радіотехніки
(повна назва)

Рівень вищої освіти – другий (магістерський)

Спеціальність 8.05090103 Радіоелектронні пристрої, системи та комплекси
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ф.Ф. Дубровка
(підпис) (ініціали, прізвище)

«23» лютого 2015 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Товкачу Ігору Олеговичу
(прізвище, ім'я, по батькові)

1. Тема дисертації Розробка структури та програмного забезпечення універсальної галузевої інтерактивної мережі з можливістю шифрування персональних даних,
науковий керівник дисертації Піддубний Володимир Олексійович. к.т.н., доц.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «11» березня 2015 р. № 298/2-с

2. Термін подання студентом дисертації 17 червня 2015

3. Об'єкт дослідження – процес обміну інформації в галузевих сайтах

4. Предмет дослідження розробка ефективного програмного забезпечення галузевого сайту з передачою шифрованих конфіденційних даних по відкритому каналу зв'язку – інтернет

5. Перелік завдань, які потрібно розробити: проаналізувати сучасні діючі CMS системи; розробити системний підхід до визначення основних задач створення інтерактивного галузевого сайту; вибрати мову програмування та програмний засіб збереження даних; реалізувати систему захисту конфіденційних даних по відкритому каналу зв'язку – інтернет; реалізувати зручний, інтуїтивно зрозумілий інтерфейс та структуровану подачу матеріалу;

розробити функціонал для об’єднання сайтів в мережу та інструменти що використовуються в мережі; реалізувати та відпрацювати програмне забезпечення в архівній галузі.

6. Орієнтовний перелік ілюстративного матеріалу електронна презентація, яка пояснює результати проведеної роботи

7. Орієнтовний перелік публікацій не менше трьох опублікованих матеріалів

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	к.т.н., доцент Каштанов С.Ф.		

9. Дата видачі завдання 23.02.2015 року

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз існуючих підходів до вирішення поставленої задачі	6.03.2015	
2	Розробка структури універсального галузевого інтеактивного сайту	17.03.2015	
3	Захист конфіденційних даних сайту при передачі їх по каналу звязку	3.04.2015	
4	Розробка функціоналу «ПОЛІДАР» NETWORK (Мережа)	17.04.2015	
5	Об’єднання сайтів в мережу, проведення та оброблення результатів дослідження	1.05.2015	
6	Охорона праці та безпека в надзвичайних ситуаціях	15.05.2015	
7	Підготовка пояснювальної записки	4.06.2015	
8	Оформлення презентації	11.06.2015	

Студент _____ І.О. Товкач
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ В.О. Піддубний
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Звіт про магістерську дисертацію: 138 с., 44 рис., 15 табл., 4 додатки, 40 джерел.

Об’єктом розробки і дослідження є процес обміну інформації в галузевих сайтах. Як предмет дослідження розглядається розробка ефективного програмного забезпечення галузевого сайту з передачою шифрованих конфіденційних даних по відкритому каналу зв’язку – інтернет. Мета роботи – дослідження і розробка структури та програмного забезпечення для створення універсальної галузевої інтерактивної мережі з можливістю передачі конфіденційних даних у шифрованому вигляді.

Проаналізовані сучасні системи створення та управленням контенту та їх можливість налаштування на галузеву специфіку. Виявлено, що жодна із проаналізованих універсальних CMS систем не задовольнає вимогам до створюваного сайту, оскільки вони мають ряд суттєвих недоліків, які виправити можливо лише через переписування значних фрагментів програмного коду самих систем.

Тому за основу було взято попередньо розроблену автором під час роботи над дипломним проектом на здобуття освітньо-кваліфікаційного рівня «бакалавр» – CMS «ПОЛІДАР». Даний функціонал модифіковано: вбудовано набір визначень взаємодії різнотипного програмного забезпечення (тобто метод абстракції API між низькорівневим та високорівневим програмним забезпеченням) та доповнено можливістю налаштування на тематичну специфіку будь-якої галузі і розгорнута в будь-яку структуру на сайті.

Розроблено функціонал «ПОЛІДАР» NETWORK, який об’єднує всі сайти в єдину мережу, і в такий спосіб забезпечує доступ до галузевих інструментів, які полегшують роботу працівників цієї галузі, та забезпечує відвідувачів високотехнологічним інструментом для пошуку інформації.

Реалізовано метод шифрування, який забезпечує конфіденційність даних при передачі по відкритому каналу зав’язку, в якому використовується симетричні алгоритми (AES, Serpent та Twofish) та асиметричний (RSA), які послідовно шар за шаром, шифрують дані, що унеможливлює несанкціонований доступ до інформації.

За допомогою одного із функціоналів системи – «ПОЛІДАР» CMS, згенеровано 62 сайти для архівних установ Київської області та об’єднано їх у спеціалізовану мережу за допомогою функціонала «ПОЛІДАР» NETWORK.

ІНТЕРАКТИВНО-КОМУНІКАЦІЙНА СИСТЕМА, ПОЛІДАР, САЙТ, NETWORK, ЗАХИСТ КОНФІДЕНЦІЙНИХ ДАНИХ, CMS

SUMMARY

Report on the master's thesis: 138 p., 44 fig., 15 tabl., 4 appl., 40 sources.

The object of research and development is the exchange of information in the branch sites. As the object of research is considered development of the effective software of the branch site with transmission of confidential data on open communication link – the Internet. Purpose of work - research and development structures and software for creation of the universal branch interactive network with the ability to transfer sensitive data in encrypted form.

The modern systems of creation and control of content and their possibility of setup on branch specifics are analyzed. It is revealed that any of the analyzed universal CMS systems doesn't meet the requirements to the created site as they have a row of essential shortcomings which can be corrected only by rewriting of the considerable fragments of a program code of systems.

Therefore, the basis was taken previously developed by the author while working on her graduate thesis on competition of educational qualification of "bachelor" – «POLIDAR» CMS. This functionality is modified: built a set of definitions of the interaction of different software components (that is, the method of abstraction API between low-level and higher-level software) and complemented by the thematic specificity of any branch and deployed to any structure on the site.

Developed functionality «POLIDAR» NETWORK, which brings together all the sites into a single network, and in this way provides access to industry tools that greatly facilitate the work of the workers in this industry, and provide visitors a high-tech tool for finding information.

Implemented encryption method, which ensures privacy of data during transmission over an open channel of communication that uses symmetric algorithms (AES, Serpent and Twofish) and asymmetric (RSA), which sequentially, layer by layer, encrypt data, making it impossible for unauthorized access to information.

By means of one of functionalities of system - "POLIDAR" CMS, it is generated the 62nd sites for archive establishments of Kiev region and are integrated them in a specialized network by means of a functionality of "POLIDAR" NETWORK.

INTERACTIVE COMMUNICATION SYSTEM, POLIDAR, SITE, NETWORK, PROTECT SENSITIVE DATA, CMS

ЗАГАЛЬНІ ВИСНОВКИ

1. Проведений аналіз існуючих систем управління сайтів, як кращих безкоштовних Joomla, eZ Publish, XOOPS, так і кращих платних Бітрікс, AMO CMS і Site Sapiens показав, що ні одна із розглянутих систем не відповідає вимогам створення інтерактивного галузевого сайту, оскільки вони мають ряд суттєвих недоліків, які виправити можливо лише через переписування значних фрагментів програмного коду самих систем, що неприйнятно.

2. Модифіковано з метою вдосконалення CMS одного із функціоналів системи «ПОЛІДАР» (попередньо розробленого автором), яка може бути налаштована на тематичну специфіку будь якої галузі та розгортати будь-яку структуру на сайті. На базі її і розроблена структура та програмне забезпечення універсального галузевого інтерактивного сайту архівної галузі.

3. Система «ПОЛІДАР» має достатню кількість гнучких функціоналів, які можуть задовільнити користувача з будь-якими вимогами, без допомоги висококваліфікованих комп’ютерних спеціалістів.

4. Побудовані для архівної галузі інфологічна та даталогічна моделі повністю задовольняють вимогам вітчизняних ДСТУ та вимогам загального міжнародного стандарту ISAD.

5. Показано, що вибрана мова програмування (PHP) та програмне забезпечення для баз даних (MSQL) відповідає вимогам, які висуваються до систем управління контентом, і можуть бути використані для створення галузевого інтерактивного сайту.

6. На основі результатів аналізу вже існуючих криптографічних алгоритмів – розроблено метод шифрування MHED-2, який використовує декілька шарів шифрування симетричними та несиметричними алгоритмами, забезпечує конфіденційність даних при передачі по відкритому каналу зав’язку та захист даних навіть при компроментації одного з них.

7. Розроблений інтерфейс є зручним та інтуїтивно зрозумілим для користувачів та працівників архівної галузі, і при цьому залишається

надзвичайно простим в обслуговуванні та не потребує допомоги комп’ютерних спеціалістів

8. Створений за допомогою запропонованої технології сайт, містить всі необхідні функціонали та інструменти, які потрібні архівній установі для якісного інформування громадськості про свою діяльність та про послуги, які можна отримати при звернення до неї.

9. За допомогою одного із функціоналів системи – «ПОЛІДАР» CMS, вже згенеровано шістдесят два сайти для архівних установ Київської області та об’єднані у спеціалізовану мережу за допомогою функціонала «ПОЛІДАР» NETWORK, які в своїй переважній більшості активно функціонують.