УДК 004.4 doi:10.20998/2413-4295.2022.04.09

РОЗРОБКА ТА ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМІЧНОЇ МОДЕЛІ ТРАНСЛЯЦІЇ ДОКУМЕНТІВ НА РІЗНОМАНІТНИХ ПРИСТРОЯХ

О. А. ТАТАРІНОВА*, О. М. МАРУСЕНКО, В. В. ІСАЄВ

Кафедра комп'ютерного моделювання процесів та систем, НТУ «ХПІ», Харків, УКРАЇНА
**e-mail: volodymyr.mietielov@khpi.edu.ua*

АНОТАЦІЯ *Спроектовано, розроблено та реалізовано веб-застосунок, призначений для трансляції електронних документів на різноманітних пристроях серед аудиторії, що знаходиться на відстані один від одного. Розроблено підходи, алгоритми та сервіс для трансляції документів різного формату на різних пристроях без використання проектора. Для побудови алгоритмів використано класичні методи стиснення та шифрування даних й паралелізму. Програмне забезпечення реалізоване мовою JavaScript з використанням фреймворків Node.js та Vue.js. Також для збереження даних користувачів використано базу даних MongoDB. Для відображення результатів роботи було розроблено сервіс для трансляції з документів різного формат у через мобільний пристрій на інші пристрої. Розроблено зручну архітектуру програмного забезпечення, яка дозволяє з легкістю підтримувати та удосконалювати сервіс у майбутньому. Реалізовано зручний та зрозумілий графічний інтерфейс для взаємодії з користувачем. Як відомо, безпосереднє використання класичних методів та алгоритмів стиснення та шифрування даних дає змогу надійно використовувати та зберігати дані користувачів. З багатьох алгоритмів було використано метод RSA. Метод RSA – це криптографічний алгоритм із відкритим ключем, заснований на обчислювальній складності задачі на множення великих цілих чисел. Також для більшої ефективності у сервісі було розроблено методи паралелізму та мікросервісну архітектуру. Мета їх полягає в тому, щоб розподілити навантаження сервісу на різні підсервіси для більшої ефективності роботи програми.*
Ключові слова: *веб-застосунок; трансляція документів; алгоритми шифрування; стиснення даних; хмарне сховище*

DEVELOPMENT AND SOFTWARE IMPLEMENTATION OF AN ALGORITHMIC MODEL FOR BROADCASTING DOCUMENTS ON VARIOUS DEVICES

O. TATARINOVA*, O. MARUSENKO, V. ISAIEV

Department of Computer Modeling of Processes and Systems, NTU "KhPI," Kharkiv, UKRAINE

ABSTRACT *The work designed, developed and implemented a web application intended for the transmission of electronic documents on various devices among the audience located at a distance from each other. The work is devoted to the development of approaches, algorithms and services for broadcasting documents of various formats on various devices without the use of a projector. Classical methods of data compression and encryption and parallelism were used to build the algorithms. The software is implemented in the JavaScript language using the Node.js and Vue.js frameworks. The MongoDB database is also used to store user data. To display the results of the work, a service was developed for broadcasting documents of various formats through a mobile device to other devices. A convenient software architecture has been developed, which allows you to easily maintain and improve the service in the future. A convenient and clear graphical interface for interaction with the user has been implemented. As you know, the direct use of classical methods and algorithms of data compression and encryption enables reliable use and storage of user data. Among many algorithms, the RSA method was used. The RSA method is a public-key cryptographic algorithm based on the computational complexity of the problem of multiplying large integers. Also, for greater efficiency in the service, parallelism methods and microservice architecture were developed. Their purpose is to distribute the load of the service on different subservices for greater efficiency of the program.*
Keywords*: web application; transmission of documents; encryption algorithms; data compression; cloud storage*

Вступ

На сьогодні методи роботи з електронними документами набувають все більшої актуальності у зв'язку з впровадженням інформаційно-комп'ютерних технологій у документообіг організації.

У зв'язку з переходом на електронний документообіг виникли три дуже важливих питання щодо аспектів зберігання та обробки електронних документів – це пошук оптимальної технології, яка надає різноманітний функціонал по роботі з документами; вибір надійного, захищеного носія інформації, що забезпечує її тривале зберігання; трансляція документів на різноманітних пристроях.

На даний момент існує декілька методів роботи з електронними документами, залежно від технології зберігання:

– зовнішні носії;

– локальний сервер чи локальний комп'ютер у створенні;

– програма електронного архіву;

– хмарна система.

Світова практика демонструє, що дедалі більше зарубіжних архівів переходить на зберігання електронних документів із застосуванням хмарних систем, що може сприяти вдосконаленню проведення презентації або прямій трансляції на будь-якому зібранні.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Використання хмарних технологій розглянуто у роботах Т.І. Вакалюк [1], питанням використання хмарних сховищ OneDrive та Dropbox присвячені дослідження І.В. Герасименко, К.І. Журавель, А.С. Паламарчук [2], огляду функціональних можливостей хмарних сервісів для створення інтерактивних мультимедійних презентацій присвячено статтю Т.В. Бондаренко [3].

Актуальність роботи обумовлена необхідністю мати можливість трансляції електронних документів при різних обставинах, маючи будь-який пристрій з виходом у мережу інтернет.

Мета роботи

Роботу присвячено розробці сервісу, призначеного для трансляції, взаємодії та презентації електронних документів через будь-який пристрій, який підключений до глобальної мережі за наявності браузеру. При цьому необхідно розробити алгоритмічну модель трансляції документів, яка буде надавати можливість надійно передавати документи зі стисненням даних.

На основі огляду методів кодування було обрано алгоритм Діффі-Хеллмана, метод RSA, арифметичне кодування та алгоритм розробки хмарного сховища.

Алгоритм арифметичного кодування було обрано у зв'язку з тим, що він має структуру алгоритму для стиснення даних без втрат. Отже використання цього методу дозволить зробити стиснення максимально ефективним, не використовуючи зайвого місця на диску.

Алгоритм Діффі-Хеллмана було обрано у зв'язку з тим, що він дає змогу двом і більше сторонам отримати спільний секретний ключ, використовуючи незахищений від прослуховування канал зв'язку.

Метод RSA було обрано у зв'язку з тим, що цей алгоритм за аналізом літературних джерел [4–8] є максимально зломостійким, ніж інші алгоритми.

Виклад основного матеріалу

Програмний засіб, розроблений для трансляції документів на різноманітних пристроях, використовує алгоритм, який складається з оновлення та перетворення даних. Він складається з трьох кроків. Першим кроком є реєстрація або вхід користувача. Другий – завантаження та зміна даних (зображень, документів тощо). На третьому кроці відбувається трансляція завантаженої інформації.

Перший етап роботи програми наведено на рис.1 за допомогою діаграми класів.

Кожен користувач — це звичайний об'єкт, розташований у базі даних MongoDB, що містить ім'я (name), адресу електронної пошти (mail), пароль (password), дату (date – потрібні нам дані) (рис. 1). Після реєстрації користувач додається до бази даних з інформацією, наведеною на рис. 2.

Відповідно до запиту (рис. 2) відбувається етап реєстрації користувача. Далі у цьому коді реалізовані параметри пароля для забезпечення безпеки (наприклад, пароль має бути не менше 6 цифр і містити великі літери та символи). Він також перевіряє ідентичність даних користувача, щоб переконатися, що немає ідентичних користувачів.

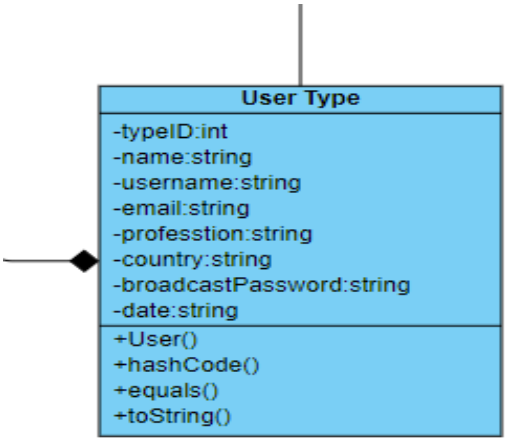

Рис. 1 – Створення користувача

Другий етап алгоритму показує як дані (зображення, документи тощо) були завантажені та змінені. За допомогою функції (рис. 3) можна додати новий файл [9].

Алгоритм пошуку та функції форматування тексту використовуються для визначення імені файлу (для подальшого використання), а сам файл та його параметри включаються у файл products.json. Для безпеки використовується шифрування md5. Крім того, у функції створюється нова папка з назвою електронної пошти користувача, і тут зберігаються всі документи, завантажені клієнтом.

Третій етап розробленого алгоритму показує яким чином транслюються завантажені дані.

Метод презентації (рис. 4) реалізує трансляцію зображення на інші пристрої. Дана система безпеки, яка використовує закритий ключ, створений самим користувачем. Іншими словами, на сеанс можуть потрапити лише запрошені гості.

Алгоритм Діффі-Хеллмана – криптографічний протокол, який дозволяє двом сторонам з парами відкритих/закритих ключів на еліптичних кривих обмінюватися секретним ключем, використовуючи несанкціонований канал зв'язку [10]. Цей секретний ключ може бути використаний як для шифрування подальшої комунікації, так і для формування нового ключа, який потім може бути використаний для подальшої комунікації з використанням симетричних алгоритмів шифрування.

Під час роботи алгоритму, кожна сторона:

1) генерує випадкове натуральне число a – закритий ключ;

2) спільно з віддаленою стороною встановлює відкриті параметри p і g; (зазвичай значення p і g генеруються на одній стороні та передаються іншій), де p є випадковим простим числом; g є першоподібним коренем за модулем p;

3) обчислює відкритий ключ A, використовуючи перетворення над закритим ключем

$$A = g^a \bmod p, \qquad (1)$$

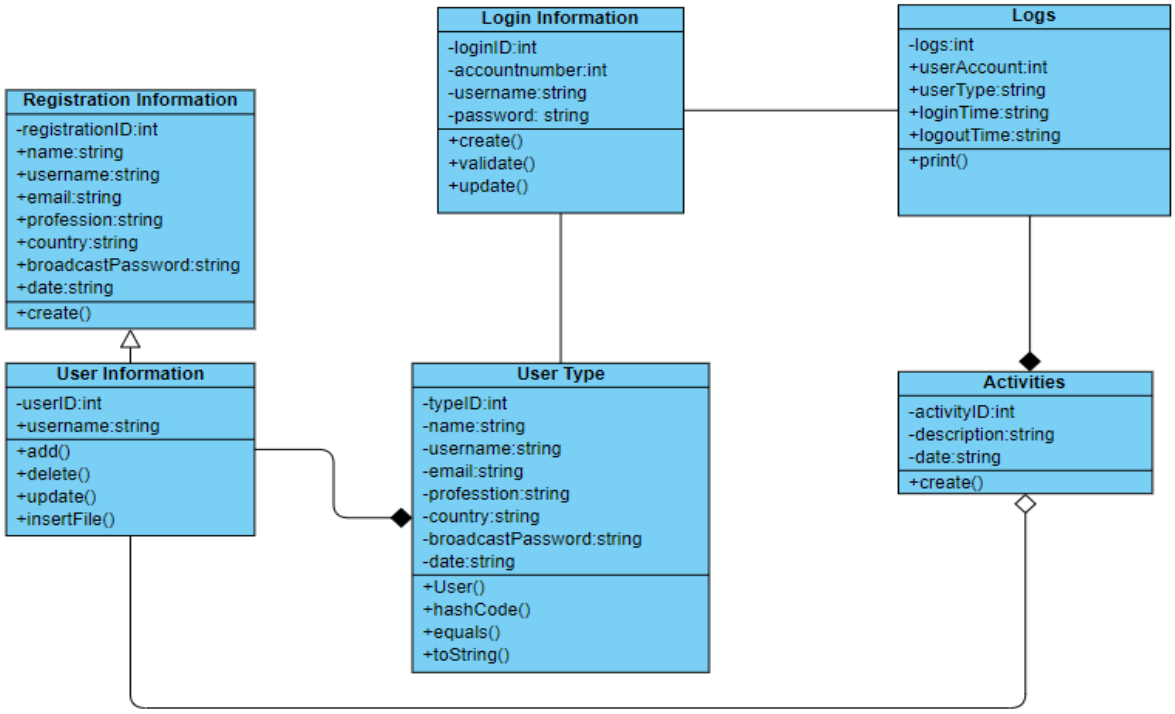

Рис. .2 – Реєстрація користувача

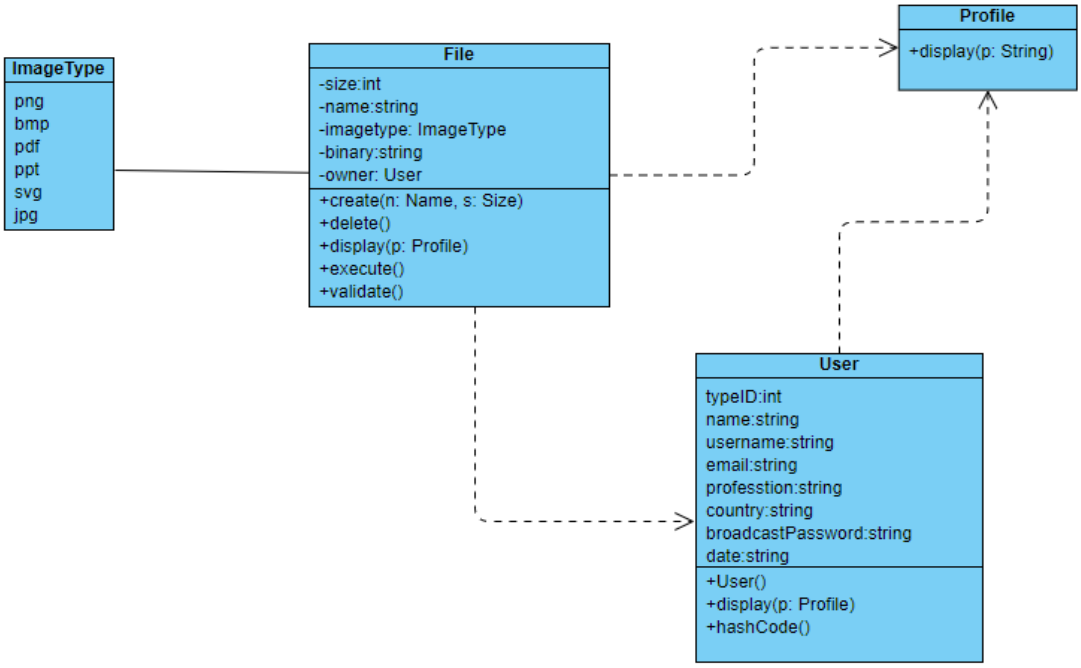

Рис. 3 – Додавання нового файлу

4) обмінюється відкритими ключами з віддаленою стороною;

5) обчислює спільний секретний ключ K, використовуючи відкритий ключ віддаленої сторони B і свій закритий ключ a

$$K = B^a \bmod p. \qquad (2)$$

Слід зазначити, що алгоритм Діффі-Хеллмана працює тільки на лініях зв'язку, які надійно захищені від змін. Якби його можна було застосувати до будь-якого відкритого каналу, це б уже усунуло проблему розподілу ключів і, можливо, замінило б всю асиметричну криптографію. Однак, якщо дані у каналі можна змінити, існує явна ймовірність того, що зловмисник «людина посередник» ввійде в процес генерації ключів, використовуючи ту саму схему, що й асиметрична криптографія.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

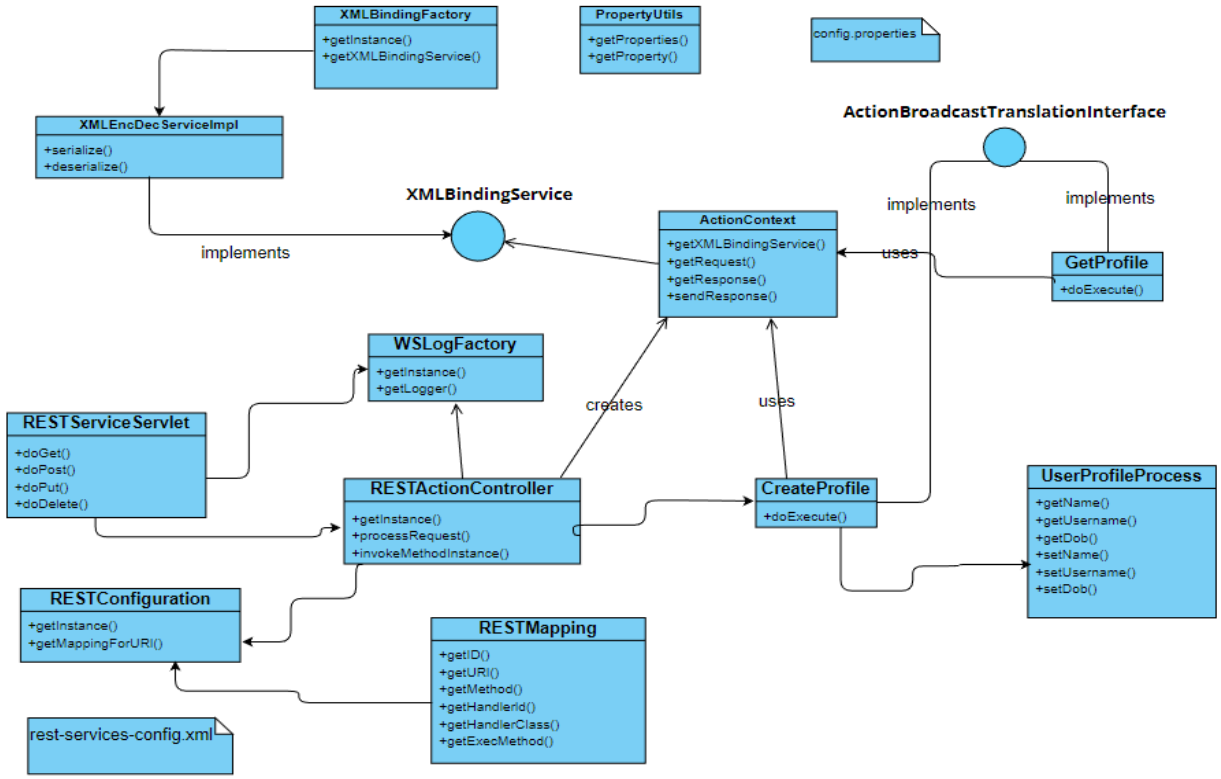

Рис. 4 – Трансляція презентації

Розроблена програмна реалізація представленої алгоритмічної моделі трансляції електронних документів орієнтована на застосування операційної системи Windows, Linux та MacOS з використанням мови програмування JavaScript. Програма використовує стандартні бекенд та фронтенд бібліотеки JavaScript, фреймворк Node.js, Express.js, Vue.js та базу даних MongoDB [11,12].

Додаток працює з вхідними даними користувача. Після того, як користувач введе свою інформацію або зареєструється у системі, він повинен вибрати, що завантажити (це може бути фото, документ тощо), а веб-додаток зберігає дані в базу даних сервісу. Зберігаючи важливі документи, файли чи іншу інформацію у кінці веб-додатку, користувач може продовжувати ним користуватися.

Для більшої наглядності роботи веб-сервісу було створено діаграму прецедентів, яка представлена на рис.5.

Для підтримки та оновлення проекту була використана SOLID архітектура – це п'ять принципів об'єктно-орієнтованого програмування, які визначають архітектуру програми: принцип єдиної відповідальності, відкритий закритий принцип, принцип підстановки Ліскова, принцип сегрегації інтерфейсу та принцип інверсії залежностей [13].

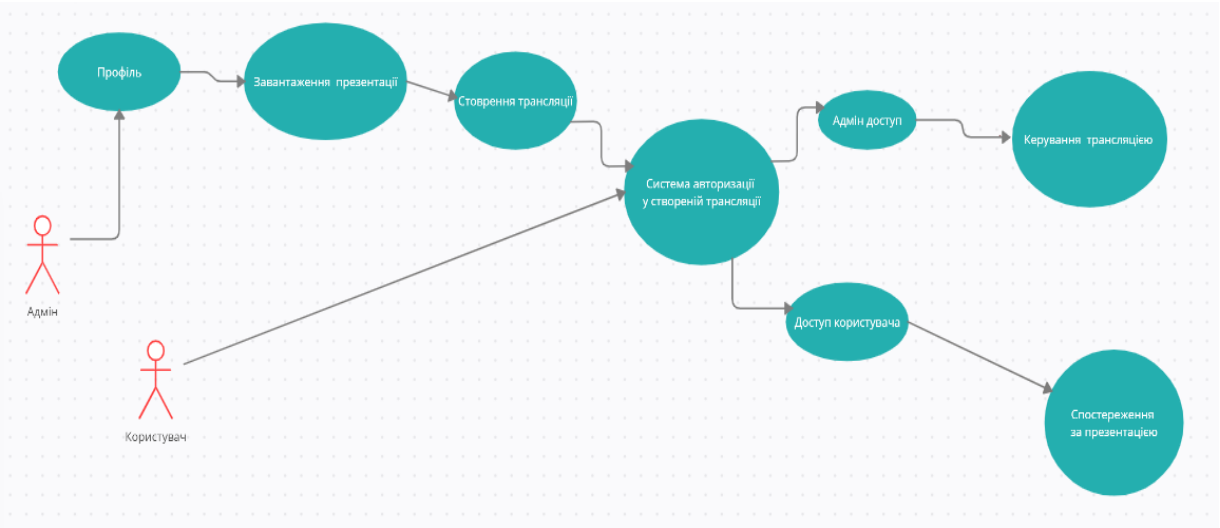

Рис. 5 – Діаграма прецедентів

Для реалізації хмарного сховища було реалізовано наступні основні функції та можливості:

– пакетне завантаження відеофайлів і зображень на S3;

– низькорівневу аутентифікацію мультимедійних файлів за допомогою кодеків;

– попередній перегляд медіафайлів;

– гнучкі параметри аутентифікації файлів;

– конфігурацію примірника на основі домену для кількох клієнтів;

– відстежування прогресу і стан збереження кожного файлу;

– підтримку плагіна JQuery-Fileupload.

Обговорення результатів

Розроблені алгоритм та програмна реалізація для трансляції та взаємодії документів різного формату на різних пристроях, в яких використано методи шифрування (алгоритм Діффі-Хелмена та алгоритми RSA і DSA) та алгоритм арифметичного кодування, також розроблені інші додаткові функції (редагування, створення аватарки, згрупувати документи, збереження, видалення тощо) для сервісу. Даний сервіс відрізняється зручною архітектурою, яка дозволяє з легкістю підтримувати та удосконалювати сервіс у майбутньому. Реалізовано зручний та зрозумілий графічний інтерфейс для взаємодії з користувачем.

Важливим етапом створення будь-якої програми є тестування. У даній роботі проведено тестування на можливі критичні ситуації. Повний цикл тестувань включає в себе: тестування системи, блоків, функціональності, зручності використання, тестування безпеки, кросбраузерне та кросплатформне тестування. Серед багатьох тестів, що використовуються, виділено конкретні тестові точки.

Також було проведено функціональне, крос-браузерне та крос-платформне тестування, щоб перевірити, як додаток працює під час роботи в різних браузерах і пристроях.

Зауважимо, що був проведений функціональний, кросбраузерний та мультиплатформений тест для перевірки, як буде вести себе веб-застосунок, якщо його запустити на різних браузерах та пристроях.

Можна відзначити, що оптимізація сервісу дозволяє користувачам насолоджуватися швидкістю запитів і роботою продукту. Цей сервіс має систему захисту від злому. Усі паролі, створені користувачем для презентацій та аккаунтів, зашифровані. Це додає додаткову безпеку додатку.

Висновки

У роботі описано підхід до програмної реалізації розробленої алгоритмічної моделі трансляції електронних документів на різноманітних пристроях, що дозволяє ефективно використовувати сервіс за рахунок розроблених методів шифрування, паралелізму та мікросервісної архітектури. Всі операції проводяться з використанням баз даних, у яких зберігаються дані користувачів та завантажені медіа файли. Програмний засіб модернізується із застосуванням алгоритмів оцінювання даних та використовується для проведення презентацій на різних пристроях.

Список літератури

1. Вакалюк Т. А. Огляд існуючих моделей хмарних послуг для використання у вищих навчальних закладах. *Тези доповідей VIII Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2016» (22–23 квітня 2016 р.).* Житомир: ЖДТУ. 2016. С. 215–217.
2. Герасименко І. В., Журавель К. І., Паламарчук О. С. Комплексне використання хмарних сервісів в електронному навчальному курсі. *Science and Education a New Dimension. Pedagogy and Psychology*. 2015. III(37). Issue 75.
3. Бондаренко Т. В. Особливості використання програмного засобу Prezi у процесі розробки навчальних презентацій. *Інформаційні технології і засоби навчання.* 2018. Том 63, №1. С. 1–11. doi:10.33407/itlt.v63i1.1907.
4. Neha Bansal, Sukhdeep Singh. RSA Encryption and Decryption System. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology.* 2020. Volume 6, Issue 5. P. 109–113. doi : 10.32628/CSEIT206520.
5. Gupta D., Biswas G., Nandan R. Security Weakness of a Lattice-based Key Exchange Protocol. *In Proceedings of the 2018 4th International Conference on Recent Advances in Information Technology.* Dhanbad, India. 15–17 March 2018. P. 1–5.
6. Priya N. and Kannan M. Comparative Study of RSA and Probabilistic Encryption. *International Journal Of Engineering And Computer Science.* 2017. Vol. 6. No 1. P. 19867–19871. doi: 10.18535/ijecs/v6i1.04.
7. Meneses F., Fuertes W., José Sancho, Salvador S., Flores D., Aules H., Castro F. Torres J., Miranda A., Nuela D. RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages. *IJCSNS International Journal of Computer Science and Network Security*. 2016. Vol. 16. No. 8. P. 55-62.
8. Abdeldaym R. S., Abd Elkader H. M., Hussein R., Modified RSA Algorithm Using Two Public Key and Chinese Remainder Theorem. *I.J. of Electronics and Information Engineering.* 2019. Vol. 10. No. 1. P. 51–64. doi: 10.6636/IJEIE.201903/51-64.
9. Cai M. A., Chervenak M. Peer-to-Peer replica location service based on a distributed hash table. *Conference: Supercomputing, Proceedings of the ACM/IEEE SC2004 Conferenc*. 2004. P. 56. doi:10.1109/SC.2004.7.
10. Noor Sattar Noor, Dalal Abdulmohsin Hammood, Ali Al-Naji, Javaan Chahl. A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication. *Computers.* 2022. 11. 3. P. 39. doi: 10.3390/computers11030039.
11. Eric Bush. *Node.js, Mongo DB, React, React Native Full-Stack Fundamentals and Beyond.* Blue Sky Productions, 2018. 394 p.
12. Amit Phaltankar, Juned Ahsan, Michael Harrison, Liviu Nedov. *MongoDB Fundamentals: A hands-on guide to using MongoDB and Atlas in the real world.* Packt Publishing Ltd, 2020. 748 p.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

13. Addy Osmani. Learning JavaScript Design Patterns: *A JavaScript and jQuery Developer's Guide*. O'Reilly Media; 1 edition (2012); Creative Commons Licensed, 2021. 254 p.

References (transliterated)

1. Vakalyuk T. A. Oglyad isnuyuchy`x modelej xmarny`x poslug dlya vy`kory`stannya u vy`shhy`x navchal`ny`x zakladax [Overview of existing models of cloud services for use in higher education institutions]. *Tezy` dopovidej VIII Mizhnarodnoyi naukovo-texnichnoyi konferenciyi «Informacijno-komp'yuterni texnologiyi – 2016» (22–23 kvitnya 2016 r.). Zhy`tomy`r. ZhDTU*, 2016, pp. 215–217 .
2. Gerasy`menko I. V., Zhuravel` K. I., Palamarchuk O. S. Kompleksne vy`kory`stannya xmarny`x servisiv v elektronnomu navchal`nomu kursi [Complex use of cloud services in an electronic training course]. *Science and Education a New Dimension. Pedagogy and Psychology,* 2015, III(37), Issue 75.
3. Bondarenko T. V. Osobly`vosti vy`kory`stannya programnogo zasobu Prezi u procesi rozrobky` navchal`ny`x prezentacij. [Peculiarities of using Prezi software in the process of developing educational presentations]. *Informacijni texnologiyi i zasoby` navchannya,* 2018, Vol. 63, no. 1, pp. 1–11, doi:10.33407/itlt.v63i1.1907.
4. Neha Bansal, Sukhdeep Singh. RSA Encryption and Decryption System. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 2020, Vol. 6, Issue 5, pp. 109–113,. doi: 10.32628/CSEIT206520.
5. Gupta D., Biswas G., Nandan R. Security Weakness of a Lattice-based Key Exchange Protocol. *In Proceedings of the 2018 4th International Conference on Recent Advances in Information Technology.* Dhanbad, India, 15–17 March 2018, pp. 1–5.
6. Priya N. and Kannan M., Comparative Study of RSA and Probabilistic Encryption. *International Journal Of Engineering And Computer Science*, 2017, Vol. 6, no 1, pp. 19867–19871, doi: 10.18535/ijecs/v6i1.04.
7. Meneses F., Fuertes W., José Sancho, Salvador S., Flores D., Aules H., Castro F. Torres J., Miranda A., Nuela D. RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages. *IJCSNS International Journal of Computer Science and Network Security*, 2016, Vol. 16, no. 8, pp. 55-62.
8. Abdeldaym R. S., Abd Elkader H. M., Hussein R., Modified RSA Algorithm Using Two Public Key and Chinese Remainder Theorem. *I.J. of Electronics and Information Engineering,* 2019, Vol. 10, no. 1, pp. 51–64, doi: 10.6636/IJEIE.201903/51-64.
9. Cai M. A., Chervenak M. Peer-to-Peer replica location service based on a distributed hash table. *Conference: Supercomputing, Proceedings of the ACM/IEEE SC2004 Conferenc*, 2004, pp. 56, doi: 10.1109/SC.2004.7.
10. Noor Sattar Noor, Dalal Abdulmohsin Hammood, Ali Al-Naji, Javaan Chahl. A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication. *Computers,* 2022, 11, 3, pp. 39, doi: 10.3390/computers11030039.
11. Eric Bush. Node.js, Mongo DB, React, React Native Full-Stack Fundamentals and Beyond. *Blue Sky Productions*, 2018. 394 p.
12. Amit Phaltankar, Juned Ahsan, Michael Harrison, Liviu Nedov. MongoDB Fundamentals: A hands-on guide to using MongoDB and Atlas in the real world. *Packt Publishing Ltd*, 2020. 748 p.
13. Addy Osmani. Learning JavaScript Design Patterns: A JavaScript and jQuery Developer's Guide. *O'Reilly Media*. 1 edition (2012). *Creative Commons Licensed*, 2021. 254 p.

Відомості про авторів (About authors)

Татарінова Оксана Андріївна – кандидат технічних наук, Національний технічний університет «Харківський політехнічний інститут», доцент кафедри комп'ютерного моделювання процесів та систем; м. Харків, Україна; ORCID: 0000-0003-3090-8469; e-mail: oksana.tatarinova@khpi.edu.ua.

Tatarinova Oksana – Ph. D., Associate Professor of the Department of Computer Modelling of Processes and Systems, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine; ORCID: 0000-0003-3090-8469; e-mail: oksana.tatarinova@khpi.edu.ua.

Марусенко Олексій Миколайович – Національний технічний університет «Харківський політехнічний інститут», асистент кафедри комп'ютерного моделювання процесів та систем; м. Харків, Україна; ORCID: 0000-0001-6911-2500; e-mail: Oleksii.Marusenko@khpi.edu.ua.

Marusenko Oleksii – Assistant of the Department of Computer Modelling of Processes and Systems, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine; ORCID: 0000-0001-6911-2500; e-mail: Oleksii.Marusenko@khpi.edu.ua.

Ісаєв Владислав Володимирович – Національний технічний університет «Харківський політехнічний інститут», студент кафедри комп'ютерного моделювання процесів та систем; м. Харків, Україна; e-mail: brodskiy.gleb@gmail.com.

Isaiev Vladyslav – Student of the Department of Computer Modelling of Processes and Systems, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine; e-mail: vladyslav.isaiev@infiz.khpi.edu.ua.

Будь ласка, посилайтесь на цю статтю наступним чином:

Татарінова О. А., Марусенко О. М., Ісаєв В. В. Розробка та програмна реалізація алгоритмічної моделі трансляції документів на різноманітних пристроях. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2022. № 4 (14). С. 59-64. doi:10.20998/2413-4295.2022.04.09.

Please cite this article as:

Tatarinova O., Marusenko O., Isaiev V. Development and software implementation of an algorithmic model for broadcasting documents on various devices. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2022, no. 4(14), pp. 59–64, doi:10.20998/2413-4295.2022.04.09.

Надійшла (received) 01.12.2022