DOI: 10.18372/2410-7840.21.14312
УДК 004.93

ШИФРУВАННЯ КОЛЬОРОВИХ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ МАТРИЦЬ АДАМАРА

Артем Фролов, Олександр Чобаль, Василь Різак

Існує безліч методів шифрування інформації. Шифрування інформації за допомогою матриць Адамара є одним із методів, які найкраще підходять для шифрування графічної інформації або інформації викладеної в формі зображень. У даній роботі було досліджено матриці Адамара та їх класифікацію, в результаті чого було визначено, що розрізняють чотири основні типи матриць Адамара: канонічні матриці Адамара (типу C), «світлі» матриці Адамара з мінімальною кількістю елементів рівних -1, матриці Адамара «50/50» з одинаковою кількістю елементів рівних 1 і -1 (тип M), напівканонічні матриці Адамара (тип D). Також було проаналізовано їх особливість і можливість у використанні у методі шифрування зображень а також особливість с кодуванням кольорових зображень. Також було визначено метод шифрування, якій використовую матриці Адамара для шифрування кольорових растрових зображень. В процесі було визначено, що достатньо використовувати неортогональні базові матриці Адамара, але в майбутньому для покращення криптостійкості застосунку можливо задіяти 16 опорних матриць Адамара розмірності 4x4. Було розроблено алгоритм шифрування комбінацій пікселів зображення з використанням матриць Адамара, а також веб-застосунок, який використовує даний метод шифрування для кодування и декодування кольорових зображень.

Ключові слова: *матриця Адамара, захист інформації, шифрування, кольорові зображення, веб-застосунок.*

Вступ. Захист інформації в сучасних комп'ютерних інформаційних системах є пріоритетним завданням. Викрадення конфіденційної інформації, знищення даних, викривлення інформації, виведення з ладу комп'ютерних систем – далеко не повний перелік усіх ризиків, що виникають у процесі експлуатації та використання сучасних інформаційних системах.

Сучасні комп'ютерні технології стали загальнодоступними і дозволяють легко відтворювати зовнішній вигляд практично будь-якого документу чи зображення. Навіть сама найскладніша поліграфія не в змозі самостійно забезпечити належний рівень захисту від підробок. У зв'язку з цим, актуальним завданням є розробка принципово нових методів захисту інформації від кіберзлочинності, ефективність яких пов'язана з використанням сучасної комп'ютерної техніки та її поєднанням з високоточними математичними методами обробки зображень.

Протягом останніх років використовувався цілий ряд методів та технологій захисту цінних паперів, зокрема лінійними та точковими періодичними та випадковими структурами, криптографічними водяними знаками, формування складних гільошних захисних сіток, побудованих на основі різних теоретичних моделей лінійних структур тощо.

Одним із методів кодування зображень являється і такий, що ґрунтується на перетворенні Адамара. Даний метод базується на принципі глобальної заміни графічного зображення кодуючими впорядкованими неперіодичними структурами, побудованими на основі ортогональних матриць Адамара без жодних ознак того чи іншого кодованого зображення та можливістю розкодовувати одним ключем різноманітні кодовані зображення. Однак в них використовується обмежена множина матриць Адамара та було відсутнє першопринципне дослідження усіх кодуючих структур на їх основі. Існує також ряд невирішених проблем, зокрема виготовлення висвітленого кодованого зображення, відтворення двох чи більше кольорових кодованих зображень, обмеження на роздільну здатність. Таким чином, розвиток сучасного методу захисту документів да зображень з використанням властивостей матриць Адамара в процесі побудови кодуючих структур є актуальним завданням для пошуку принципово нових рішень в області кодування інформації. [1]

Метою роботи є:

1. Провести аналіз сучасного стану технологій кодування з використанням матриць Адамара;
2. Досліждення класифікації матриць Адамара розмірності 4x4;
3. Розроблення методу захисту саме кольорових зображень з використанням кодуючих структур Адамара;
4. Розробка програмного забезпечення що реалізує метод захисту кольорових зображень.

Об'єктом дослідження є технологічний процес виготовлення форм кодованого зображення для технології захисту інформації збереженої на

кольорових зображеннях на основі впорядкованих неперіодичних кодуючих структур Адамара.

Предметом дослідження є методи, способи та алгоритми формування кодуючих структур Адамара, технологічні параметри та умови виготовлення форм кодованих зображень, створення нової інформаційної технології захисту кольорових зображенн, яка забезпечує високий рівень захисту.

Дослідження матриць Адамара. Матриці Адамара являють собою ортогональні квадратні матриці, елементи яких можуть приймати значення тільки (+1) та (-1). Серед множини матриць Адамара розмірності можна виділити чотири типи. До першого з них належать канонічні матриці Адамара (типу С), в яких всі елементи одного рядка і одного стовпця рівні 1. Типовим прикладом є симетрична канонічна матриця Адамара. Другий тип включає матриці Адамара «50/50» з одинаковою кількістю елементів рівних 1 і -1 (тип М). Прикладом такої матриці є подібна матриця Адамара (рис.1). Окрім вказаних двох типів існують «світлі» матриці Адамара з мінімальною кількістю елементів рівних -1. Прикладом є діагональна матриця Адамара (тип L). В роботі підтверджено наявність четвертого типу ортогональних матриць Адамара. За ознаками структури стовпців ці матриці відповідають канонічному типу матриць Адамара. Проте за ознаками структури рядків вони не належать до жодного з означених вище типів матриць (типу С, М та L). Перший стовпець, що містить 4 елементи, характеризується співвідношенням «3/1», тобто має 3 світлих елементи і 1 темний, а наступні три стовпці – співвідношеннями «1/3». Групу матриць з такою структурою рядків/стовпців названо в роботі «напівканонічними» матрицями Адамара (тип D) (рис. 1). Темними комірками позначені елементи -1, а елементам 1 відповідають світлі комірки.

Класифікація за ознакою подібності множини всіх ортогональних матриць Адамара розмірності дозволила виявити більш загальні властивості таких матриць для пошуку нових ефективних методів кодування графічних зображень.

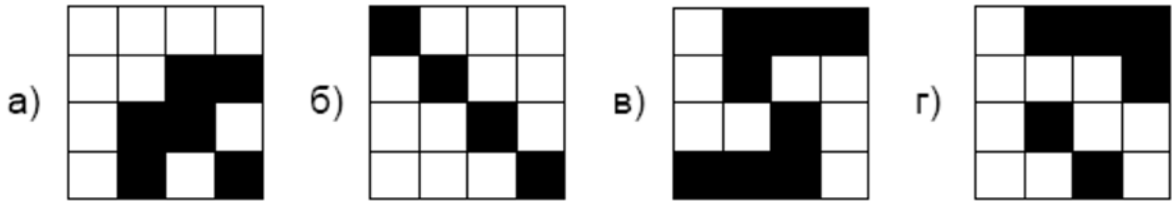

Рис. 1. Типи базових матриць Адамара

Розрізняють чотири основні типи матриць Адамара (Рис. 1):

а. Канонічні матриці Адамара (типу С), в яких всі елементи одного рядка і одного стовпця рівні 1. Типовим прикладом є симетрична канонічна матриця Адамара H_C.

б. «Світлі» матриці Адамара з мінімальною кількістю елементів рівних -1. Прикладом є діагональна матриця Адамара H_L (тип L).

в. Матриці Адамара «50/50» з одинаковою кількістю елементів рівних 1 і -1 (тип М). Прикладом такої матриці є S-подібна матриця Адамара.

г. Напівканонічні матриці Адамара (тип D). Перший стовпець, що містить 4 елементи, характеризується співвідношенням «3/1», тобто має 3 світлих елементи і 1 темний, а наступні три стовпці – співвідношеннями «1/3».

Метод кодування зображень. Метод кодування базується на основі кодуючих структур Адамара. Спосіб виготовлення графічного елементу захисту зображень полягає в тому, що з вхідного зображення формують кодоване зображення з використанням спеціальної комп'ютерної програми, за допомогою якої вхідне зображення перетворюють у багаторівневе графічне зображення, кожен рівень якого замінюють матрицею комірок впорядкованої неперіодичної структури. Для розшифрування програма накладає кодоване зображення і ключ кодованого зображення одне на одного, точно сумістивши їх. Внаслідок цього кодоване зображення та його ключ позволяють відновити закодоване зображення, колір якого може бути відмінний від кольорів кодованого зображення та ключа, але достатньо наближеним до оригіналу щоб опрацювати інформацію (рис. 2).

Алгоритм кодування кольорових зображень складається з наступних кроків:

1. Зберегти в масив дані кожного пікселя кольорового зображення (R, G, B).

2. Створити зображення-ключ з випадково розставленими кольоровими кодуючими структурами Адамара.

3. Створити закодоване зображення базуючись на кольорі пікселя секретного зображення та зображенні-ключі.

4. Повторювати крок 3 для кожного пікселя секретного зображення до отримання шифрованого зображення.

5. Після накладання закодованого зображення на зображення-ключ, секретне зображення може бути розшифроване людським зором.

Рис. 2. Принципова схема кодування зображень

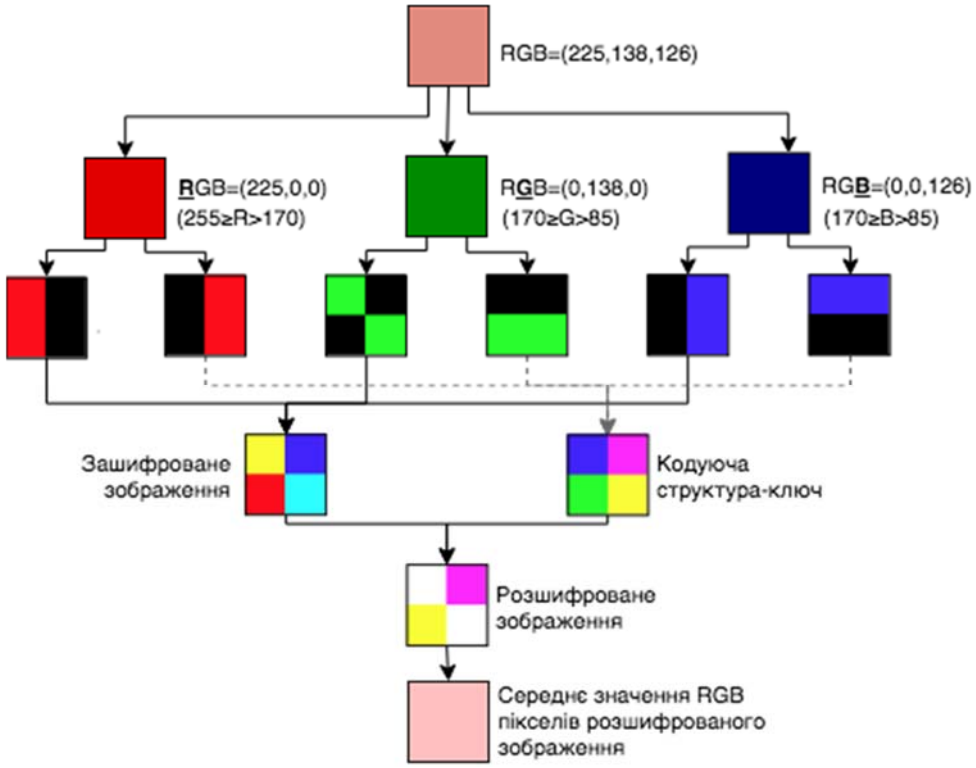

Рис. 3. Схема поділу кольорового пікселя

Кодування вхідного зображення виконується за принципом глобальної заміни рівнів багаторівневого бінаризованого зображення блоками матриць комірок з впорядкованою неперіодичною структурою. В результаті цього на кодованому зображенні різні рівні заповнюють блоками матриць комірок з відповідною впорядкованою неперіодичною структурою, яка забезпечує візуальну нерозрізнимість ліній рівнів цього зображення. Для розкодовування зображення формують ключ, який містить одну з кодуючих структур кодованого зображення. В результаті суміщення ключа з кодованим зображенням взаємодоповнюючі блоки базових матриць комірок двох кодуючих структур перекриваються пропорційно до величини рівня і таким чином відновлюється закодоване зображення із вдвічі більшою роздільною здатністю. [13]

На рис. 4 приведено 16 опорних матриць Адамара розмірності 4x4, які складаються з 4 неортогональних базових матриць та містять однакову кількість елементів 1 та -1.

Зображення, яке слід закодувати, бінаризується, причому кожним чотирьом суміжним пікселям у відповідність ставиться впорядкована неперіодична структура, еквівалентна до однієї з опорних матриць Адамара розмірності, кожна з яких в свою чергу складається з 4 базових матриць розмірності.

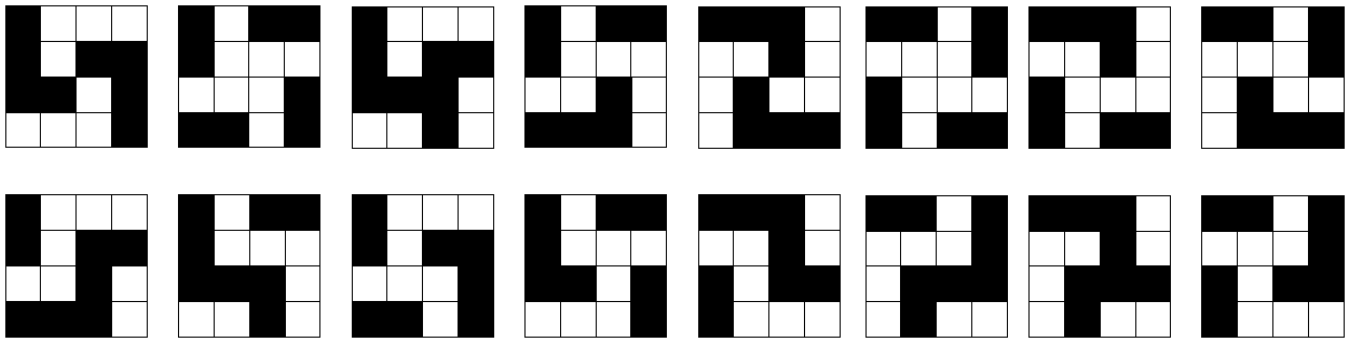

Рис. 5. Базові матриці Адамара

При розробці веб-застосунку було використано неортогональні базові матриці Адамара, але в майбутньому для покращення криптостійкості застосунку можливо задіяти 16 опорних матриць Адамара розмірності 4x4 наведених вище. [3]

Розроблений застосунок.

Було розроблено веб-застосунок який працює наступним чином:

1. Користувач повинен обрати зображення із файлової системи яке потрібно закодувати;
2. При натисненні кнопки «Зашифрувати» програма опрацьовує зображення і за допомогою методу шифрування с використанням матриць Адамара створює закодоване зображення та ключ;
   a. В процесі створення закодованого зображення для кожного пікселя зображення спершу визначається випадковим чином три матриці Адамара (по одній для кожного кольору R, G і B). Випадковим чином вони обираються із 6 можливих.
   b. Для кожної матриці закодованого зображення відповідно підбирається матриця-ключ. Матриця ключ генеруються таким чином, щоб при накладанні одної матриці на другу вони утворювали комбінацію із чотирьох пікселів які максимально наближені до пікселя вхідного/секретного зображення.
   c. Матриці R, G і B одного пікселя закодованого зображення накладаються одне на одного. Теж саме відбувається с матрицями R, G і B ключа.
   d. Далі дані матриці додаються до закодованого зображення і зображення ключа відповідно до позиції пікселя який вони мають відтворити.
   e. В результаті користувач веб-застосунку отримує два зображення (закодоване зображення и ключ). За допомогою лише одного з них неможливо відтворити секретне зображення.
3. При натисненні кнопки «Розшифрувати» програма накладає закодоване зображення на ключ і результат відображає в секції «Розкодоване зображення».

Рис. 4. Веб-застосунок для кодування та декодування кольорових зображень

Висновки. У даній роботі було досліджено можливість використання матриць Адамара для шифрування кольорових зображень. Даний метод шифрування інформації є ефективним способом

протидії несанкціонованому викраденню інформації кіберзлочинцями. У роботі було створено інформаційну технологію захисту кольорових зображень на основі кодуючих структур Адамара, яка забезпечує високий рівень захисту.

Було проведено аналіз сучасного стану технології цифрової обробки оптичної інформації для захисту документів та зображень та обґрунтовано необхідність розробки елементів захисту у вигляді кодованих графічних зображень із захисними ознаками. Визначено напрямок розвитку сучасних технологій захисту кольорових зображень на основі використання впорядкованих неперіодичних структур Адамара та спеціалізованого програмного забезпечення.

Також було розроблено загальний алгоритм кодування кольорового зображення шляхом глобальної заміни зображення впорядкованою неперіодичною структурою Адамара, що забезпечує високу однорідність і візуальну нерозрізнимість кодованих зображень та використано RGB колірну модель для шифрування.

Розроблено веб-застосунок для шифрування кольорових зображень на базі мови Javascript.

ЛІТЕРАТУРА

[1]. Л. Дідух, М. Шовгенюк, Н. Писанчин, "Комп'ютерні методи обробки зображень для сучасних технологій захисту цінних паперів", *Комп'ютерні технології друкарства*, №15, С. 175-187, 2006.

[2]. Л. Дідух, М. Шовгенюк, "Класи подібних матриць Адамара", *Комп'ютерні технології друкарства*, №22, С. 54-64, 2010.

[3]. М. Шовгенюк, Л. Дідух, *Класи подібних матриць Адамара та їх властивості*, Львів, 2009, 18 с (Препринт / ІФКС НАН України, ICMP-09-11U).

[4]. C. Swenson, *Modern Cryptanalysis: Techniques for Advanced Code Breaking*, Indianapolis, Wiley, 2008, 264 p.

[5]. H. Evangelaras, "Applications of Hadamard matrices", *Journal of Telecommunications and Information Technology*, pp. 3-10, 2003.

[6]. D. Stinson, *An introduction to visual cryptography, presented at Public Key Solutions* '97, Toronto, Canada, April 28–30, 1997.

[7]. G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, "Visual cryptography for general access structures, Inform", *Comput. 129,* pp. 86-106, 1996.

[8]. G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, *Extended schemes for visual cryptography*.

[9]. C. Blundo, A. De Santis, D.R. Stinson, "On the contrast in visual cryptography schemes", *J. Cryptology*, Vol. 12, pp. 261-289, 1999.

[10]. V. Rijmen, B. Preneel, "Ecient colour visual encryption for shared colors of Benetton", *Eurocrypto'96*, Rump Session, Berlin, 1996.

[11]. A. Rubin, "Independent one-time passwords", Comput. Systems, no. 9, pp. 15-27, 1996.

[12]. A. Shamir, "Visual cryptanalysis", *Proceedings of the Euro- crypt'98*, Espoo, 1998.

[13]. C. Poynton, Frequently asked questions about color. [Electronic resource]. Available: http://www. inforamp.net/~poynton.

ШИФРОВАНИЯ ЦВЕТНЫХ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ МАТРИЦ АДАМАРА

Существует множество методов шифрования информации. Шифрование информации с помощью матриц Адамара является одним из методов, которые лучше всего подходят для шифрования графической информации или информации изложенной в форме изображений. В данной работе были исследованы матрицы Адамара и их классификация, в результате чего было установлено, что различают четыре основных типа матриц Адамара: канонические матрицы Адамара (типа С), «светлые» матрицы Адамара с минимальным количеством элементов равных -1, матрицы Адамара «50/50» с одинаковым количеством элементов равных 1 и 1 (тип М), полу-канонические матрицы Адамара (тип D). Также были проанализированы их особенность и возможность в использовании в методе шифрования изображений, а также особенность кодировки цветных изображений. Также были определен метод шифрования, которой использую матрицы Адамара для шифрования цветных растровых изображений. В процессе было установлено, что достаточно использовать неортогональные базовые матрицы Адамара, но в будущем для улучшения криптостойкости приложения возможно задействовать 16 опорных матриц Адамара размерности 4х4. Был разработан алгоритм шифрования комбинаций точек изображения с использованием матриц Адамара, а также веб-приложение, которое использует данный метод шифрования для кодирования и декодирования цветных изображений.

Ключевые слова: матрица Адамара, защита информации, шифрование, цветные изображения, веб-приложение.

ENCRYPTION OF COLOR IMAGES USING HADAMARD MATRICES

There are many methods of encrypting information. Encrypting information using Hadamard matrices is one of the methods that is best for encrypting graphic information or information in the form of images. In this paper, the Hadamard matrices and their classification were investigated, and it was determined that there are four main types of Hadamard matrices: the canonical Hadamard matrices (type C), the "light" Hadamard matrix with a minimum number of elements equal to -1, the Hadamard matrix "50 / 50 "with equal number of elements equal to 1 and -1 (type M), semi-canonical Hadamard matrix (type D). Also their feature and ability to use in the image encryption method were analyzed, as well as the feature with color

image encoding. An encryption method that used the Hadamard matrix to encrypt color raster images was identified. In the process, it was determined that it was sufficient to use non-orthogonal Hadamard base matrices, but in the future, 16 Hadamard 4x4 support matrices could be used to improve the crypto-stability of the application. An algorithm for encrypting image pixel combinations using the Hadamard matrices was developed. First, for each pixel of the image, this method randomly determines three Hadamard matrices R, G and B. Then, for each matrix of the encoded image, a matrix key is selected. The key matrix is generated in such a way that when you overlay one matrix on another, they form a combination of four pixels that are as close as possible to the pixel of the input / secret image. The R, G, and B matrices of one pixel of the encoded image and key overlap. The matrix data is then added to the encoded image and key image respectively according to the pixel position. As a result, the web application user receives two images (encoded image and key). Only one of them cannot play a secret image. A web application was developed that uses this encryption method to encode and decode color images.
Keywords: Hadamard matrix, information security, encryption, color images, web application.

Фролов Артем Олександрович, аспірант кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.
E-mail: artem.frolov@uzhnu.edu.ua.
Orcid ID: 0000-0003-4967-0067.
Фролов Артем Александрович, аспирант кафедры твердотельной электроники и информационной безопасности физического факультета УжНУ.
Frolov Artem, PhD student, Department of Solid State Electronics and Information Security of the Physics Faculty, UzhNU.

Чобаль Олександр Ілліч, кандидат фізико-математичних наук, доцент кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.
E-mail: oleksandr.chobal@uzhnu.edu.ua.
Orcid ID: 0000-0002-8042-8052.
Чобаль Александр Ильич, кандидат физико-математических наук, доцент кафедры твердотельной электроники и информационной безопасности физического факультета УжНУ.
Chobal Oleksandr, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Solid State Electronics and Information Security of the Physical Faculty, UzhNU.

Різак Василь Михайлович, доктор фізико-математичних наук, професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.
E-mail: vrizak@uzhnu.edu.ua.
Orcid ID: 0000-0002-9177-0662.
Ризак Василий Михайлович, доктор физико-математических наук, профессор, заведующий кафедрой твердотельной электроники и информационной безопасности физического факультета УжНУ.
Rizak Vasyl, Doctor of Physical and Mathematical Sciences, Professor, Head of the Department of Solid State Electronics and Information Security of the Physical Faculty, UzhNU.

DOI: 10.18372/2410-7840.21.14338
УДК 004.056.53

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ВПЛИВУ ТА МЕТОДІВ ПРОТИДІЇ ФІШИНГУ

Дмитро Мехед, Юлія Ткач, Володимир Базилевич

У статті проаналізовано актуальні загрози інформаційній безпеці та зроблено прогноз основних напрямків проведення кібератак в майбутньому. З'ясовано, що серед існуючих загроз інформаційній безпеці вже котрий рік поспіль перші позиції займають методи соціальної інженерії. Виділено найбільш поширені інструменти і методи однієї зі складових соціальної інженерії - фішингу, зокрема вспливаючі вікна, міжсайтовий скриптинг, помилки URL-адреси тощо. Дослідниками сформульовано низку рекомендацій щодо захисту організацій та підприємств у контексті використання ефективних технічних засобів захисту (наприклад, SIEM-рішення - для своєчасного виявлення атаки, якщо інфраструктура виявилась зараженою, автоматизовані засоби аналізу захищеності і виявлення вразливостей в ПЗ, мережевий екран рівня додатків (web application firewall) як превентивний захід захисту веб-ресурсів), безпосереднього захисту даних (зокрема, збереження конфіденційної інформації у закритому вигляді з обмеженим доступом, регулярне створення резервних копії систем і збереження їх на виділених серверах окремо від мережевих сегментів робочих систем), а також безпеки персоналу (а саме, підвищення обізнаності працівників в питаннях ІБ, регулярне навчання персоналу правилам безпечної роботи в Інтернеті, пояснення методів атак і способів захисту тощо).
Ключові слова: *інформаційна безпека, соціальна інженерія, фішинг, засоби захисту інформації.*