пристроїв у складі пари мережі вузлів квантової мережі. Попередньо розподілені ключі, створюються з використанням датчика випадкових чисел, з вузлів квантової мережі, з доставкою довіреним кур'єром до нового вузла квантової мережі. Після проведення успішного сеансу квантового розподілення ключів з новим вузлом квантової мережі, даний вузол вважається підключеним до квантової мережі протоколу квантового розподілення ключів.

3. Класичні квантові ключі захисту квантово-захищених ключів для проведення розподілу квантово-захищених ключів для систем захисту інформації-користувачів можуть бути використані квантово-захищені ключі, розподілені із захистом на квантових ключах по квантовій мережі протоколу квантового розподілення ключів між новим вузлом квантової мережі та необхідними цільовими вузлами квантової мережі.

Запропоновано архітектуру квантової мережі квантового розподілення ключів змішаної топології, та наведені вимоги до функцій квантової мережі, отримані на основі запропонованих підходів розподілу квантово-захищених ключів та виявлених, при цьому, особливостей квантових пристроїв. Така квантова мережа надає можливість розподіляти квантово-захищені ключі, передавати згенеровані ключі у пари систем захисту інформації-користувачів, на основі запитаного системами захисту інформації-користувачами забезпечення ключами, вирішуючи задачу зміни та доставки ключів шифрування.

1. Квантова криптографія. Пояснення [Електронний ресурс] // Quantum Xchange. – 2019. – Режим доступу: https://quantumxc.com/blog/quantum-cryptography-explained/ (дата звернення 02.03.2024).
2. Satish Kumar. Quantum Cryptography [Електронний ресурс] // Tutorialspoint. – 2023. – Режим доступу: http://surl.li/fjebs (дата звернення 05.03.2024).

A study of methods for detecting hidden threats in multimedia objects on web resources

UDK 004.056.5:004.932

Dmytro Denysiuk[1], Bohdan Savenko[2]

Khmelnytskyi National University,
[1]denysiuk@khmnu.edu.ua, [2]savenko_bohdan@ukr.net

Multimedia objects on web resources are not only interface elements or user-generated content, but also potential carriers of hidden cyber threats. Mechanisms for loading images, video files, avatars, banners, and graphic containers create a separate attack surface that often falls outside the scope of traditional web request scanning. Hidden data can be embedded in the pixel area, frequency coefficients, EXIF/XMP metadata, service segments, overlay areas, or polyglot files [1, 2].

The problem is that such modifications do not always alter the appearance of the multimedia object and may not violate the format’s basic characteristics. Therefore, checking only the file extension, MIME type, signature, or antivirus database does not

provide sufficient reliability in detection. For web resources, this creates a risk of bypassing download filters, covertly transmitting service markers, storing script fragments, or preparing multi-stage attacks [1, 3].

The main groups of features characterizing hidden cyber threats in multimedia objects of web resources have been identified, and the feasibility of their comprehensive use within the framework of multimodal analysis has been determined. Formally, a multimedia object is presented as a multi-level information container:

$$M = \{P, F, S, Meta, B\}, \quad (1)$$

where M is a multimedia object of a web resource; P is a pixel matrix or a sequence of frames; F is a set of frequency features; S are structural elements of the file container; $Meta$ is EXIF/XMP metadata; B are behavioral features recorded during the opening, decoding, previewing, or transformation of the object.

Model (1) provides a formalized description of a multimedia object as a container comprising heterogeneous groups of features. Component P reflects changes in the pixel domain, particularly those characteristic of LSB steganography; F describes anomalies in the frequency domain, specifically in DCT or DWT coefficients; S characterizes the integrity of the file structure, the consistency of signatures, MIME type, and actual content; Meta covers hidden or atypical service fields; B reflects behavioral manifestations that arise during the processing of the object in a controlled environment.

To detect hidden threats, it is advisable to use statistical, structural, frequency-based, neural network, and behavioral methods. Statistical analysis is used to study entropy, histograms, correlations between pixels, and noise residuals. It is effective for detecting some steganographic changes, but depends on the compression method, image quality, and type of hiding [3].

Structural analysis makes it possible to verify whether a container conforms to the declared format, as well as to detect redundant data, duplicate signatures, anomalous service blocks, suspicious metadata, and polyglot structures [2]. Frequency analysis is used to detect changes in DCT and DWT representations, which is relevant for JPEG images and other lossy compression formats. Neural network methods enable the automatic extraction of complex latent features that are difficult to formalize manually.

Behavioral analysis complements static analysis by allowing us to assess how the software environment reacts to a suspicious object. In a sandbox, honeypot, or decoy environment, it is possible to capture events that do not occur during a standard file analysis but arise when the file is opened, decoded, previewed, or transformed.

For practical application in web security, it is advisable to develop a comprehensive risk assessment:

$$R(M) = w_1 A_{stat} + w_2 A_{struct} + w_3 A_{freq} + w_4 A_{nn} + w_5 A_{beh} \quad (2)$$

where $R(M)$ - the overall risk of a multimedia object; A_{stat} - statistical anomalies; A_{struct}- structural abnormalities; A_{freq}- frequency deviations; A_{nn}- evaluation of a neural network detector; A_{beh}- behavioral abnormalities; w_1, w_2, w_3, w_4, w_5 - weighting factors for the respective groups of characteristics.

A multimodal model makes it possible to assess a multimedia object as a potential carrier of a cyber threat by taking into account a set of heterogeneous features, including pixel-based, frequency-based, structural, metadata-related, and behavioral characteristics. Such representation allows the object to be analyzed not only as an image, video, or graphic file, but also as a complex information container in which hidden modifications may appear at different levels.

To protect web resources, it is advisable to combine statistical, structural, frequency-based, neural network, and behavioral methods within an integrated risk assessment framework. This combination increases the reliability of detecting hidden modifications in multimedia content, since each group of methods covers a specific class of indicators and compensates for the limitations of the others.

This approach reduces the detection system's reliance on a single type of indicator and enables it to respond more effectively to various methods of concealing threats. As a result, the assessment of multimedia content becomes more comprehensive and better adapted to the detection of hidden cyber threats in web environments.

1. Almehmadi L., Basuhail A., Alghazzawi D., Rabie O. Framework for Malware Triggering Using Steganography. Applied Sciences. – 2022. – Vol. 12, No. 16. – Article 8176. DOI: https://doi.org/10.3390/app12168176
2. Koch L., Oesch S., Chaulagain A., Adkisson M., Erwin S., Weber B. Toward the Detection of Polyglot Files. Proceedings of CSET 2022 – 15th Workshop on Cyber Security Experimentation and Test. – 2022. – P. 120–128. DOI: https://doi.org/10.1145/3546096.3546106
3. Denysiuk D., Savenko O., Lysenko S., Savenko B., Kashtalian A. Method for Detecting Steganographic Changes in Images Using Machine Learning. Proceedings of the 2023 IEEE 13th International Conference on Dependable Systems, Services and Technologies (DESSERT). – Athens, Greece, 2023. – P. 1–6. DOI: https://doi.org/10.1109/DESSERT61349.2023.10416453

Optimizing uav routes under conditions of restricted access to confidential objects

UDC 623.746.4-519:004

Юлія Ткач[1], Ігор Дюба[2]

Національний університет "Чернігівська політехніка",
[1]tkachym79@gmail.com, [2] idyuba@gmail.com

Introduction. Modern scenarios for the use of Unmanned Aerial Vehicles (UAVs) require solving complex routing problems in dynamic environments. This issue becomes particularly acute when planning flights over territories containing restricted access objects or critical infrastructure. Traditional approaches based on the complete bypass of "No-Fly Zones" lead to significant time and energy expenditures.

Problem Statement. This study considers the applied task of constructing a UAV route from point A to point C through a transit area B. Area B contains objects whose coordinates are confidential. It is necessary to minimize the travel time while ensuring