На початковому етапі роботи інформаційно-аналітичної системи список формується експертним шляхом, із загальної кількості форумів тематичних інтернет – ресурсів виділяються ті, тематика яких дозволяє інтернет - інформацію віднести до хакерських (інформація містить результати спеціалізованих досліджень з виявлення вразливостей та загроз інформаційної безпеки конфіденційних даних, повідомлення про комп'ютерні атаки, вразливості, шкідливе програмне забезпечення). Автоматизоване виявлення нових форумів тематичних інтернет-ресурсів, в даній ситуації, можливо, шляхом проведення аналізу різноманітних форумів інтернет-ресурсів, з використанням запропонованих критеріїв відбору текстових повідомлень, що належать до заданої предметної області, для якої проводиться аналіз з використання онтології [2]. Для реалізації фізичної системи, потрібно реалізувати в матеріальні сутності всі елементи логічного представлення.

Для фізичного представлення моделі використовується діаграма UML розгортання, відображається загальна топологія та конфігурація інформаційно-обчислювальної системи, а також розподіл за окремими вузлами компонентів. Вузлами діаграми інформаційно-обчислювальної системи є персональний комп'ютер користувача, сервер адміністратора.

Покращення якості прогнозування виникнення вразливостей та загроз безпеки інформації з використанням систем логічного нечіткого виводу може сприяти збільшення кількості вхідних змінних, використанню більш точних нечітких правил продукцій, також велике значення має визначення функцій приналежності вихідних та вхідних параметрів системи логічного нечіткого виводу, необхідно враховувати статистичні показники потоку текстових повідомлень форумів тематичних інтернет-ресурсів.

1. Ленков С.В**.** Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів / С.В. Лєнков, В.М. Джулій, А.М. Берназ, І.В. Муляр, І.В. Пампуха // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2023. – Вип. №78. – С. 123-134.
2. Ленков С.В. Метод протидії поширенню та виявлення шкідливої інформації в соціальних мережах/ С.В. Ленков, В.М. Джулій, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №77. – С. 103-117.

## Структура мережі розподілу квантово-захищених ключів у мережах магістральної топології

УДК 004.056

Володимир Джулій[1], Максим Вовкович[2]

*Хмельницький національний університет, [1]dzhuliivm@khmnu.edu.ua, [2]maksym.vovkovyhc@gmail.com*

На основі запропонованих вимог до структури мережі та методу розподілу квантово-захищених ключів у мережах магістральної топології сформована архітектура квантової мережі квантового розподілення ключів змішаної топології.

Квантова мережа квантового розподілу ключів будується на основі довірених вузлів мережі, до кожного з вузлів можуть підключатися системи захисту інформації-користувачі, зовнішні пристрої. Кожен вузол квантової мережі щонайменше містить один напівкомплект квантових пристроїв і з'єднаний щонайменше квантовим каналом зв'язку не менш ніж із одним сусіднім вузлом квантової мережі [1].

Кожен вузол квантової мережі квантового розподілу ключів містить один і більше модулів генерації квантових ключів мережі, реалізованих квантовими пристроями. На даний момент через відсутність стандартизованого протоколу квантового розподілу ключів між двома кінцях квантового каналу мережі повинні розташовуватися пристрої, реалізовані одним виробником і виконувати один протокол квантового розподілу ключів. На кожному сегменті квантової мережі квантового розподілу ключів можливе застосування різних квантових пристроїв.

Максимальна довжина квантового каналу квантової мережі кожного сегмента визначається граничними значеннями втрат на обраному сегменті протоколу квантового розподілу ключів квантового каналу.

Для початку роботи квантової мережі розподілу ключів, початку генерації квантових ключів для розподілу квантово-захищених ключів необхідно розподілити попередньо відповідні набори ключів: на пари сусідніх вузлів квантової мережі; для аутентифікації квантових пристроїв класичного каналу.

Розподіл квантово-захищених ключів між парами мережі вузлів квантової мережі реалізується відповідно до запропонованого методу. Обчислення магістральної підмережі квантової мережі проводиться вузлом, на який надійшов запит квантово-захищеного ключа з урахуванням топології мережі квантового розподілу ключів [2].

Для визначення пар мережі цільових вузлів квантової мережі, на які розподіляються квантово-захищені ключі відповідно до запиту системою захисту інформації - користувача, необхідно підтримувати базу відповідності підключених систем захисту інформації-користувачів і вузлів квантової мережі в актуальному стані для всієї квантової мережі. Ідентифікація мережі вузлів квантової мережі повинна бути унікальною для визначення, однозначно, цільових вузлів квантової мережі. Мережа протоколу квантового розподілу ключів може будуватися підключенням нових вузлів квантової мережі ітераційним шляхом до існуючої квантової мережі протоколу квантового розподілу ключів. Для підключення до мережі нового вузла квантової мережі необхідно:

1. Під’єднати вузол квантової мережі до квантового каналу мережі. Квантовий канал під’єднаний може бути до до вузла квантової мережі, до комутатора, до модуля генерації квантових ключів мережі.

2. Завантажити в новий вузол квантової мережі, попередньо згенеровані розподілені ключі для побудови в мережі автентифікованого каналу квантових

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