УДК 681.324

СОВРЕМЕННЫЕ ПОДХОДЫ К БЕЗОПАСНОЙ ПЕРЕДАЧЕ ДАННЫХ: ВЫБОР НЕЙРОСЕТИ ДЛЯ ГЕНЕРАЦИИ ИЗОБРАЖЕНИЙ, МЕТОДЫ ШИФРОВАНИЯ И ФОРМАТ JSON

Елисеев А.В.

Рязанский государственный радиотехнический университет,
г. Рязань, Российская Федерация

Научный руководитель: Бакулева М.А. – к.т.н., доцент, доцент кафедры САПР ВС

Аннотация. Данная работа посвящена исследованию современных подходов безопасной передачи данных на основе выбора нейросети для генерации изображений, методов шифрования, а также использования формата передачи данных JSON. В статье рассматривается применение нейросети Kandinsky для создания изображений по текстовому описанию, а также проводится анализ надёжности алгоритмов шифрования данных SHA3-224 и AES.

Ключевые слова: шифрование, конфиденциальность данных, безопасная передача данных, Kandinsky, SHA3-224, AES, JSON

Введение. В современном мире информационные технологии играют важную роль в жизни человека, вопросы безопасности данных приобретают ещё более значимый характер [1].

В данной статье рассматриваются основные аспекты методов шифрования данных, информационной безопасности, а также средства защиты информации.

Основная часть. Информационная безопасность представляет собой область, характерной чертой которой является защита конфиденциальности, доступности и целостности данных. При увеличении роста объёма информации, хранимой и передаваемой в цифровом формате, обеспечение безопасности данных становится всё более значимой. Кибератаки, утечка данных способны привести к серьёзным последствиям для частных лиц и крупных компаний.

Шифрование является одним из основных методов обеспечения безопасности хранимой информации. Шифрованием является процесс преобразования исходных данных в вид информации, нечитаемый для посторонних с целью защиты её от несанкционированного доступа. В практике используется достаточно широкий список методов шифрования. Существует классический вид, такой как шифр Цезаря и Виженера. В крупных организациях используются зачастую современные алгоритмы, такие как AES (Advanced Encryption Standard) и RSA (Rivest-Shamir-Adleman).

RSA - это криптографический асимметричный алгоритм, который используется для шифрования подписи данных.

Наиболее распространённый подход – использование симметричного алгоритма шифрования AES. Спектр его использования охватывает защиту данных в таких областях, как финансы, телекоммуникации и здравоохранение [2]. Он функционирует за счёт замены байтов и перемешивании столбцов и строк матрицы данных с использованием ключа шифрования.

SHA3-224 – алгоритм хэширования, использующийся для проверки целостности данных. Хэширование представляет собой строку фиксированной длины из различных входных данных. Хеш способен меняться при изменении входных данных. Данная особенность позволяет обнаружить какие-либо изменения, а также повреждения.

В качестве примера автором было предложено создать эмулированные данные в формате объекта JSON, в полях которого и будет задействован алгоритм хэширования SHA3-224, а также симметричный алгоритм шифрования AES (рисунок 1):

```
export const clients_information = [
  [
    {
      userId: '70a0a38d9a3c2e8b5e06f4f3a7c6b1d1',
      id: 1,
      clientsPhoto: './pictures/clients-photos/person1.png',
      fingerprint_data: 'f8b2d0b0aef4d6b9c8e1c836c1b5b0d4e1f8e76f9f2d9c4f3e79f2d9',
      clients_iris_data:'E3rXcJx0tKoW2uN6qW9V7w',
      name: 'James',
      surname: 'Smith',
      eye_color: 'gray' ,
    },
```

Рисунок 1 – Объект JSON с зашифрованными данными о пользователе

Ключи рассматриваемого объекта имеют следующую расшифровку:

1. userID – зашифрованный уникальный идентификатор клиента;
2. id – порядковый номер клиента;
3. clientsPhoto – поле, где указан путь до папки, в которой находятся сгенерированные изображения пользователя;
4. fingerprint_data – результат вычисления хэш-функции, шифрующей данные об отпечатке пальца человека;
5. clients_iris_data – результат вычисления хэш-функции, шифрующей данные о радужке глаза пользователя;
6. eye_color – цвет глаз пользователя;
7. name – имя пользователя;
8. surname – фамилия пользователя.

Для того, чтобы воссоздать изображения человека необходимо воспользоваться нейросетью. Выбор был сделан в пользу нейросети Kandinsky, исходя из ряда преимуществ. Нейросеть способна генерировать изображения с нуля по текстовому запросу на 101 языке и создавать картинки в разных стилях, начиная от фотореализма, заканчивая рисованными иллюстрациями. Также Kandinsky может использоваться для редактирования изображений и соединять несколько картинок в одну. Ещё одним достоинством данной нейросети является достраивание картинки: когда нейросеть Kandinsky сгенерировала изображение, она может дорисовать что-нибудь сверху, снизу, справа, слева [3].

В ходе генерирования изображения по текстовому описанию были получены следующие картинки (рисунок 2) и (рисунок 3):

Рисунок 2 – Сгенерированное изображение женщины с помощью нейросети Kandinsky

Рисунок 3 – Сгенерированное изображение мужчины с помощью нейросети Kandinsky

Таким образом были получены примеры эмулированных зашифрованных данных с помощью алгоритмов SHA3-224 и AES. А также сгенерированные изображения пользователей с помощью нейросети Kandinsky.

Заключение. Проведён и выполнен анализ алгоритмов шифрования данных. Важно отметить, что защита конфиденциальности, целостности и доступности информации является важной составляющей работы частных лиц, государств, больших и малых организаций. Использование современных методов хэширования, шифрования способны эффективно справляться с угрозами информационной безопасности.

Важно помнить о том, что безопасность информации – постоянный процесс, требующий постоянной адаптации к новым угрозам.

Информационная безопасность должна быть приоритетом для всех участников цифрового мира, чтобы была возможность обеспечить конфиденциальность и сохранность данных в условиях постоянно меняющейся киберугрозы.

Список литературы

1. Информационные технологии [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Информационные_технологии. Дата доступа: 24.03.24.

2. Алгоритмы шифрования, на которых держится мир [Электронный ресурс]. Режим доступа: https://thecode.media/5-encrypts/. Дата доступа: 24.03.24.

3.«Кандинский»: как пользоваться нейросетью «Сбера» [Электронный ресурс]. Режим доступа: https://skillbox.ru/media/design/kandinskiy-kak-polzovatsya-neyrosetyu-sbera/. Дата доступа 24.03.24.

UDC 681.324

MODERN APPROACHES TO SECURE DATA TRANSMISSION: CHOOSING A NEURAL NETWORK FOR IMAGE GENERATION, ENCRYPTION METHODS AND JSON FORMAT

Eliseev A.V.

Ryazan State Radio Engineering University, Ryazan, Russian Federation

Bakuleva M.A. – Cand. of Sci., associate professor, associate professor of the department of CAD Computing

Annotation. This work is devoted to the study of modern approaches to secure data transmission based on the choice of a neural network for image generation, encryption methods, as well as the use of the JSON data transmission format. The article discusses the use of the Kandinsky neural network to create images based on a text description, and also analyzes the reliability of the SHA3-224 and AES data encryption algorithms.

Keywords: encryption, data privacy, secure data transfer, Kandinsky, SHA3-224, AES, JSON