CLAIMS

1. A method for detecting suspicious users in messaging systems performed on a computing device, wherein in accordance with this method:

receiving multiple user messages from at least one messaging system;

analyzing each of the received user messages to identify at least one sign of suspiciousness of a message from a given set of signs of suspiciousness of messages;

if the at least one sign of suspiciousness of the message is identified in the analyzed user message, identifying at least one user associated with the analyzed user message in the specified messaging systems;

assigning each of the identified users a grade of suspiciousness depending on the identified signs of suspiciousness of the message, each identified sign of suspiciousness contributing to the assigned grade of suspiciousness, ensuring a change in a value of a reputation indicator of the identified user based on the assigned grade of suspiciousness; and

classifying the users in at least one of the messaging systems as suspicious users in the event if the changed value of their reputation indicator exceeds a predetermined reputation threshold limit.

2. The method of claim 1, further comprising:

identifying a description format of the received user messages; and

if the identified description format does not correspond to a unified data description format suitable for the computing device, converting the received messages into the unified data description format.

3. The method of claim 1, further comprising:

detecting voice messages and videos in the received user messages; and

converting the voice messages and the videos into text.

4. The method of claim 1, wherein analyzing each of the received user messages comprises performing at least one of following substages:

- detecting in the analyzed user message of at least one malicious link;

- detecting of at least one malicious payment system account in the analyzed user message;

- detecting in the analyzed user message of at least one malicious email address; and

- detecting in the analyzed user message of at least one malicious account in a financial institution.

5. The method of claim 4, wherein detecting the at least one malicious link in the analyzed user message comprises:

extracting at least one reference from the analyzed user message; and

performing at least one of:

- analyzing a domain name of the extracted reference for harmfulness using at least one analysis technique;

- obtaining at least one file located at the extracted reference, and analyzing the at least one file for harmfulness using at least one analysis technique; and

- receiving html-code of a web resource located at the extracted reference, analyzing the html-code for harmfulness using at least one analysis technique.

6. The method of claim 5, further comprising establishing whether the extracted at least one reference coincides at least partially with one of known malicious links.

7. The method of claim 5, wherein analyzing the domain name for harmfulness comprises establishing whether the analyzed domain name coincides at least in part with one of known malicious domain names.

8. The method of claim 5, wherein analyzing the obtained at least one file located at the extracted reference for maliciousness comprises calculating a hash sum of the at least one file, and establishing whether the calculated hash sum of the analyzed file coincides with a hash sum of one of known malicious files.

9. The method of claim 5, wherein analyzing the received html-code of the web resource comprises conducting a search in the received html-code for specified keywords indicating malicious nature of the web resource.

10. The method of claim 4, wherein detecting the at least one malicious payment system account in the analyzed user message comprises:

extracting at least one payment system account from the analyzed user message ; and

determining a match of the extracted at least one payment system account with one of known malicious payment system accounts.

11. The method of claim 4, wherein detecting the at least one malicious email address in the analyzed user message comprises:

extracting at least one email address from the analyzed user message; and

determining a match of the extracted email address with one of known malicious email addresses.

12. The method of claim 1, further comprising:

analyzing identification data of the identified users in order to identify at least one suspiciousness sign of the user from a given set of suspiciousness signs of users; and

assigning an additional grade of suspiciousness to each of the identified users, depending on the identified suspiciousness signs of the message, each detected suspiciousness sign contributing to the assigned additional grade of suspiciousness, ensuring the change in the value of the reputation indicator of the said user based on the assigned additional grade of suspiciousness.

13. The method of claim 12, wherein analyzing the identification data comprises analyzing the identification data with respect to only those identified users whose reputation indicator exceeds a specified minimum reputation threshold, which is less than the predetermined reputation threshold limit.

14. Method of any of claims 12-13, wherein identifying the at least one suspiciousness sign of each of the identified users comprises performing at least one of:

- establishing whether an avatar, full name and / or nickname of the identified user matches a corresponding information of an administrator in at least one of the messaging systems;

- detecting whether the identified user is a program that simulates a user behavior of the user in the corresponding messaging system;

- detecting whether at least one of the persons invited by the identified user to exchange messages within the framework of at least one message exchange channel in the corresponding messaging system is a program that simulates a user behavior in the specified messaging system; and

- detecting whether there is at least one user in the messaging systems with identification data that matches the identification data of the identified user.

15. The method of claim 14, wherein detecting whether the identified user is a program that simulates the user behavior in the corresponding messaging system comprises:

analyzing an activity of sending messages by the specified user in the specified messaging system for a specified period of time; and

if it is found out that the activity of sending messages by the user corresponds to a specific timing scheme, classifying the specified user as the program that simulates the user behavior.

16. The method of claim 1, wherein identifying the at least one user associated with the analyzed user message in the specified messaging systems comprises:

detecting messages that are similar to the analyzed user message in these messaging systems, ensuring the association of users who sent such similar messages to a group of related users; and

if the reputation indicator of at least one of the users in the group of related users exceeds the predetermined reputation threshold limit, classifying all users from the group of related users as suspicious users.

17. The method of claim 1, wherein identifying the at least one user associated with the analyzed user message in the specified messaging systems comprises:

detecting users with similar identification data in these messaging systems by ensuring that such users are combined into a group of related users; and

if the reputation indicator of at least one of the users in the group of related users exceeds the predetermined reputation threshold limit, classifying all users from the group of related users as suspicious users.

18. The method of claim 1, wherein identifying the at least one user associated with the analyzed user message in the specified messaging systems comprises:

establishing a possible link between references extracted from the messages being analyzed in the messaging systems with other references extracted from the messages being analyzed in these messaging systems, with a provision of an integration of such users who sent similar messages into a group of interconnected users when establishing such link; and

if the reputation indicator of one of the users in the group of interconnected users exceeds the predetermined reputation threshold limit, classifying all users from the group of interconnected users as suspicious users.

19. The method of claim 18, wherein establishing the link between the references extracted from the analyzed messages in the messaging systems comprises establishing, for each pair of references, at least one of:

- whether domain names have a similar spelling;
- whether domain names are registered to a same person;
- whether same personal data are specified for registered domain names;
- whether domain names are located at a same IP address; and
- whether extracted references have a same “URL”.

20. The method of claim 1, further comprising sending information about each of the suspicious users to the appropriate messaging system.

21. The method of claim 1, further comprising sending a request to block each of the suspicious users to the appropriate messaging system.

22. The method of claim 1, further comprising saving the analyzed user messages to a user message database located on the computing device.

23. The method of claim 22, further comprising, for at least one of the saved user messages, sending a request to the appropriate messaging system associated with the saved user message to establish whether the user has changed the user message in the specified messaging system, wherein, if it is established that the user message has changed, receiving the changed user message from the specified messaging system with provision of its re-analysis for signs of suspiciousness.

24. The method of claim 23, wherein sending the request comprises sending the request to the messaging system for at least one saved user message associated with a user whose reputation indicator has exceeded a minimum reputation threshold.

25. The method of claim 22, further comprising, for at least one of the saved user messages, accessing, via a computing device, the corresponding messaging system to retrieve a user message from its message base, attributes of which match attributes of the saved user message; calculating hash sums of the saved user message and the retrieved user message; and, in the event of a mismatch of the calculated hash-sums, carrying out a repeated analysis of the specified changed user message for signs of suspiciousness.

26. The method of claim 25, wherein accessing the corresponding messaging system to retrieve the user message from its message base is carried out for at least one saved user message that is associated with a user whose reputation indicator has exceeded a minimum reputation threshold.

27. The method of claim 1, further comprising blocking the identified suspicious users in the respective messaging systems by means of a computing device.

28. A computing device for detecting suspicious users in messaging systems, configured to communicate with messaging systems and comprising memory for storing machine-readable instructions and at least one computing processor configured to execute the machine-readable instructions ensuring the implementation of a method for detecting suspicious users in messaging systems according to any of claims 1-27.