CLAIMS

1. A computing device configured to detect malicious domain names in network traffic in real time, the computing device comprises:

a communication module configured to receive network traffic from a data network,

a filtering module, configured to connect to the communication module to receive the network traffic from the communication module and to perform at least the following:

extracting a plurality of data packets from the received network traffic,

analyzing said extracted data packets, ensuring the extraction of at least one domain name from said plurality of data packets,

an analyzing module, configured to connect to the filtering module to receive the specified domain names from the filtering module and to analyze each of the obtained domain names using a given set of analysis methods, ensuring that a given numerical value is assigned to each of a given set of features of a domain name suspiciousness corresponding to one of the given set of analysis methods, for each analyzed domain name, depending on the results of its analysis using the specified analysis methods,

a processing module, configured to connect to the analyzing module to receive from the analyzing module the indicated features of suspiciousness with the assigned numerical values for each domain name and with the possibility of analyzing them using a specified set of analysis rules ensuring that each domain name is classified as malicious domain names, if the received results of the analysis of features of suspiciousness are characteristic of malicious domain names.

2. The computing device of claim 1, wherein the communication module is further configured to connect to at least one of the network traffic capture devices connected to the data network.

3. The computing device of claim 1, wherein the filtering module is further configured to determine if there is an analytical report for each of the extracted domain names.

4. The computing device of claim 3, wherein, in response to a presence of the analytical report, the filtering module is configured to perform at least the following operations:

receiving data on analytical reports,

establishing the correspondence of each of the extracted domain names to one of the available analytical reports using character-by-character comparison of each of the extracted domain names with domain names that identify analytical reports in the indicated obtained data.

5. The computing device of claim 3 or 4, wherein, in response to an absence of the analytical report for the extracted domain name, the filtering module is additionally configured to transfer the specified domain name to the analysing module.

6. The computing device of claim 1, wherein, when analyzing the obtained domain names, the analyzing module is configured to perform at least the following operations:

determining the number of characters in each of the received domain names,

determining whether a certain number of characters correspond to each analyzed domain name given the threshold value of the length of the domain name,

assignment of a given numerical value to a suspiciousness attribute of a domain name, representing the length of the domain name being analyzed, depending on the result of establishing compliance.

7. The computing device of claim 6, wherein, when analyzing the obtained domain names, the analyzing module is additionally configured to perform at least the following operations:

getting a set of known domain names,

establishing the coincidence of each of the extracted domain names with one of the known domain names using character-by-character comparison of each of the extracted domain names with domain names in the obtained set of domain names,

assignment of a given numerical value to another feature of a domain name suspiciousness, representing popularity of the analyzed domain name, depending on the result of establishing a match.

8. The computing device of claim 7, wherein, when analyzing the obtained domain names, the analyzing module is additionally configured to perform at least the following operations:

determining the frequency of occurrence of each of the many N-grams in each of the obtained domain names, each N-gram corresponding to a combination of N consecutive characters,

determining the entropy of the N-gram of the specified analyzed domain name as a function of the specific frequency of occurrence of each N-gram in this analyzed domain name,

comparison of the determined entropy of the N-gram of the analyzed domain name with the specified threshold value of the entropy of the N-gram,

assignment of a given numerical value to another feature of a domain name suspiciousness, representing entropy of the analyzed domain name, depending on the result of the comparison.

9. The computing device of claim 8, wherein, when analyzing the obtained domain names, the analyzing module is additionally configured to perform at least the following operations:

getting data about language dictionaries,

extracting at least one word from each of the received domain names,

matching each of the specified extracted words with one of the words in the language dictionaries from the specified received data,

assignment of a given numerical value to another feature of a domain name suspiciousness, representing meaningfulness of the analyzed domain name, depending on the result of establishing a match.

10. The computing device of claim 9, wherein, when analyzing the obtained domain names, the analyzing module is additionally configured to perform at least the following operations:

getting data about language dictionaries,

extracting at least one word from each of the received domain names,

determining the Levenshtein distance between each of the specified extracted words and the corresponding one of the words in the language dictionaries of the specified obtained data,

comparison of a certain Levenshtein distance with a predetermined threshold value

assignment of a given numerical value to another feature of a domain name suspiciousness, representing correctness of spelling of the analyzed domain name, depending on the result of the comparison.

11. The computing device of claim 1, wherein the analyzing module is further configured to change the given set of analysis methods.

12. The computing device of claim 1, wherein, in response to assigning a domain name to malicious domain names, the processing module is further configured to issue a warning message, block network traffic from infected devices and/or create an analytical report for the malicious domain name.

13. The computing device of claim 10, wherein the processing module is configured to analyze the obtained set of features of suspiciousness of the analyzed domain name using at least one previously trained machine-learning algorithm.

14. The computing device of claim 1, wherein the analyzing module is further configured to receive, via the communication module, at least one domain name from at least one source of domain names.

15. A method to detect malicious domain names in network traffic in real time implemented by a computing device, the method comprising:

receiving, using a communication module of the computing device, network traffic from a data network,

extracting, using a filtering module of the computing device, a plurality of data packets from the received network traffic,

analysing, using the filtering module, said extracted data packets, ensuring the extraction of at least one domain name from said plurality of data packets,

analysing, using an analyzing module of the computing device, obtained domain names, using a given set of analysis methods, ensuring that a given numerical value is assigned to each of a given set of features of a domain name suspiciousness corresponding to one of the given set of analysis methods for each analyzed domain name depending on the results of its analysis using the specified methods of analysis,

analysing, using a processing module of the computing device, obtained features of a domain name suspiciousness with the assigned numerical values using a specified set of analysis rules with ensuring that each domain name is classified as malicious domain names, if the results of the analysis of features of suspiciousness are characteristic of malicious domain names.

16. The method of claim 15, wherein the step of receiving network traffic further comprises connecting, using the communication module, to at least one of the network traffic capture devices included in the data network.

17. The method of claim 15, wherein, for the extracted domain names, it is further determined by the filtering module whether there is an analytical report for each of these extracted domain names.

18. The method of claim 17, wherein the step of detecting the presence of the analytical report includes performing, by the filtering module, at least the following sub-steps:

receiving data on analytical reports,

establishing the correspondence of each of the extracted domain names to one of the available analytical reports using character-by-character comparison of each of the extracted domain names with domain names that identify analytical reports in the indicated obtained data.

19. The method of claim 17, wherein, in response to the absence of analytical report for the extracted domain name, the specified domain name is transmitted to the analyzing module using the filtering module.

20. The method of claim 15, wherein the step of analyzing the obtained domain names comprises performing, with the analyzing module, at least the following sub-steps:

determining the number of characters in each of the received domain names,

determining whether a certain number of characters correspond to each analyzed domain name given the threshold value of the length of the domain name,

assignment of a given numerical value to a suspiciousness attribute of a domain name, representing the length of the domain name being analyzed, depending on the result of establishing compliance.

21. The method of claim 20, wherein the step of analyzing the obtained domain names comprises performing, with the analyzing module, at least the following sub-steps:

getting a set of known domain names,

establishing the coincidence of each of the extracted domain names with one of the known domain names using character-by-character comparison of each of the extracted domain names with domain names in the obtained set of domain names,

assignment of a given numerical value to another feature of a domain name suspiciousness, representing popularity of the analyzed domain name, depending on the result of establishing a match.

22. The method of claim 21, wherein the step of analyzing the obtained domain names comprises performing, with the analyzing module, at least the following sub-steps:

determining the frequency of occurrence of each of the many N-grams in each of the obtained domain names, each N-gram corresponding to a combination of N consecutive characters,

determining the entropy of the N-gram of the specified analyzed domain name as a function of the specific frequency of occurrence of each N-gram in this analyzed domain name,

comparison of the determined entropy of the N-gram of the analyzed domain name with the specified threshold value of the entropy of the N-gram,

assignment of a given numerical value to another feature of a domain name suspiciousness, representing entropy of the analyzed domain name, depending on the result of the comparison.

23. The method of claim 22, wherein the step of analyzing the obtained domain names comprises performing, with the analyzing module, at least the following sub-steps:

getting data about language dictionaries,

extracting at least one word from each of the received domain names,

matching each of the specified extracted words with one of the words in the language dictionaries from the specified received data,

assignment of a given numerical value to another feature of a domain name suspiciousness, representing meaningfulness of the analyzed domain name, depending on the result of establishing a match.

24. The method of claim 23, wherein the step of analyzing the obtained domain names comprises performing, with the analyzing module, at least the following sub-steps:

getting data about language dictionaries,

extracting at least one word from each of the received domain names,

determining the Levenshtein distance between each of the specified extracted words and the corresponding one of the words in the language dictionaries of the specified obtained data,

comparison of a certain Levenshtein distance with a predetermined threshold value

assignment of a given numerical value to another feature of a domain name suspiciousness, representing correctness of spelling of the analyzed domain name, depending on the result of the comparison.

25. The method of claim 15, wherein the given set of analysis methods is further modified by the analyzing module.

26. The method of claim 15, wherein, in response to assigning a domain name to malicious domain names, the method further comprises, using the processing module, issuing an alert message, blocking network traffic from infected devices and/or creating an analytical report for the malicious domain name.

27. The method of claim 24, wherein the step of analyzing the features of suspiciousness includes analyzing, with the processing module, the obtained set of features of suspiciousness of the analyzed domain name using at least one previously trained machine-learning algorithm.

28. The method of claim 15, wherein according to the analyzing module, a plurality of domain names from at least one source of domain names are additionally obtained via the communication module.

29. Machine-readable medium for long-term storage of data storing machine-readable instructions that, when executed by a computing device, cause the execution of the steps of the method of any of claims 15-28.