УДК 004.855.5
DOI: 10.26102/2310-6018/2022.38.3.011

# Обнаружение угроз безопасности информации с использованием глубоких нейронных сетей в компьютерных сетях в режиме реального времени

**С.Г. Клюев, Е.Е. Трунов**✉

*Краснодарское высшее военное училище,*
*Краснодар, Российская Федерация*
*ittehnology2018@gmail.com*✉

***Резюме.*** В настоящее время вопрос обнаружения угроз безопасности информации в компьютерных сетях становится проблемой, когда речь заходит о предупреждении таких угроз в реальном времени. Растет количество абонентов практически любой компьютерной сети, а вместе с этим и количество угроз, которые могут привести к возникновению реальной опасности функционирования сети. В связи с этим требуется наличие современных механизмов, которые позволят своевременно, близко к реальному времени реагировать на возникающие угрозы безопасности информации. В данной работе проведен анализ возможных механизмов защиты от угроз нарушения безопасности в компьютерных сетях, и предложена методика реализации такой защиты с использованием нейронных сетей. Кроме того, реализован контрольный пример с обученной глубокой нейронной сетью, которая способна обнаруживать угрозы безопасности информации с высокой точностью и минимальными задержками. Материалы статьи представляют практическую ценность при внедрении такой нейронной сети в систему обнаружения вторжений. Предложенным в статье методом можно добиться близкого к реальному времени реагированию на угрозы нарушения безопасности информации и, как следствие, предотвратить возможные инциденты информационной безопасности.

***Ключевые слова:*** компьютерная сеть, нейронная сеть, угроза нарушения безопасности, глубокое обучение, механизм защиты.

***Для цитирования:*** Клюев С.Г., Трунов Е.Е. Обнаружение угроз безопасности информации с использованием глубоких нейронных сетей в компьютерных сетях в режиме реального времени. *Моделирование, оптимизация и информационные технологии*. 2022;10(3). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1212. DOI: 10.26102/2310-6018/2022.38.3.011

# Detection of information security threats using deep neural networks in computer networks in real time

**S.G. Klyuev, E.E. Trunov**✉

*Krasnodar Higher Military School,*
*Krasnodar, Russian Federation*
*ittehnology2018@gmail.com*✉

***Abstract.*** Currently, the issue of detecting information security threats in computer networks is becoming a problem when it comes to preventing such threats in real time. The number of subscribers of almost any computer network is growing and so does the number of threats that can create a potential danger to the functioning of the network. In this regard, modern mechanisms that will help to respond to emerging information security threats in a timely manner are required. In this paper, the analysis of possible mechanisms of protection against security threats in computer networks is carried out and a methodology for implementing such protection using neural networks is proposed. In addition, a control example is implemented with a trained deep neural network which is able to detect information security

 

threats with high accuracy and minimal delays. The materials of the article are of practical value when incorporating such a neural network into an intrusion detection system. By means of the method proposed in the article, it is possible to achieve a near-real-time response to information security threats and, as a result, prevent possible information security accidents.

***Keywords:*** computer network, neural network, security threat, deep learning, protection mechanism.

***For citation:*** Klyuev S.G., Trunov E.E. Detection of information security threats using deep neural networks in computer networks in real time. *Modeling, Optimization and Information Technology*. 2022;10(3). Available from: https://moitvivt.ru/ru/journal/pdf?id=1212. DOI: 10.26102/2310-6018/2022.38.3.xxx (In Russ.).

## Введение

На сегодняшний день нейросетевые технологии стали неотъемлемой частью практически любого программного обеспечения. Область их применения настолько широка, что они используются в распознавании изображений, анализе больших объемов данных, оптимизации, прогнозировании, системах помощи принятия решений и во многих других областях. Не обошли стороной нейронные сети и сферу информационной безопасности. Комплексные программные продукты для защиты информационных систем уже имеют в своем составе самообучающиеся нейронные сети, которые показывают высокие показатели в точности и скорости принятия решений.

Такие нейронные сети спустя время могут с высокой вероятностью прогнозировать возможные угрозы безопасности информации, даже при условии того, что они никогда прежде с ними не сталкивались.

Большое количество угроз нарушения безопасности в компьютерных сетях объясняется в первую очередь множеством управляющих механизмов, в качестве которых могут выступать как аппаратные, так и программные средства. Все это множество классифицируется по уровням, объектам воздействия и последствиям, к которым они могут привести.

Основные уровни угроз и их характеристики в компьютерных сетях показаны в Таблице 1.

Таблица 1 – Угрозы нарушения безопасности
Table 1 – Security threats

| Уровни угроз | Объект воздействия | Последствия |
|---|---|---|
| Программный уровень | Управляющее программное обеспечение | 1. Несанкционированный доступ и сбор информации.<br>2. Фальсификация данных.<br>3. Уничтожение данных.<br>4. Вывод устройств из строя.<br>5. Заражение устройств вредоносным программным обеспечением |
| Сетевой уровень | Узлы сети | 1. Нарушение маршрутизации.<br>2. Изменение топологии сети.<br>3. Вывод узлов из строя |

Можно заметить, что проявления различных угроз в компьютерных сетях очень разнообразно. Из этого можно сделать вывод, что специалисту, разрабатывающему программное обеспечение, придется прописывать сигнатурное поведение для каждой отдельно взятой угрозы. Это влечет за собой огромный объем работы для программиста

и это без учета появления новых угроз, которые ему в данный момент неизвестны. Зная это и то, как работают нейронные сети, можно найти единственно верное решение – использование нейронных сетей. Они позволят не прописывать каждую угрозу отдельно, а дать на обучение конечный набор обучающих данных, по которым нейронная сеть сможет со временем принимать самостоятельные решения, основываясь на уже известных. Таким образом, мы можем заложить в программу функцию прогнозирования, что будет особенно полезно, когда конечное множество угроз неизвестно или они постоянно обновляются, что де-факто всегда и происходит.

На сегодняшний день обнаружение угроз в компьютерных сетях происходит с использованием SIEM-систем или систем обнаружения вторжений как надстройки для антивирусов и сетевого оборудования. Такой подход не позволяет эффективно прогнозировать события, происходящие в компьютерных сетях. В первую очередь это связано с тем, что SIEM-системы используют уже сформированный банк данных об угрозах, а в случае с постоянно изменяющейся структурой сети сбор такой информации не дает высокой вероятности правильного прогнозирования. В качестве альтернативы предлагается применение интеллектуальных методов глубокого обучения. Основной концепцией данного подхода является построение глубокой нейронной сети и дальнейший процесс ее обучения.

Данная работа посвящена разработке такой глубокой нейронной сети, которая позволит эффективно и в режиме близкого к реальному времени обнаруживать и прогнозировать возможные угрозы нарушения безопасности информации. Цель работы состоит в том, чтобы создать нейронную сеть, которая с высокой точностью будет способна обнаруживать определенные классы угроз нарушения безопасности, которые могут возникать в компьютерной сети. Для достижения поставленной цели необходимо:

1) сформировать достаточный для тренировки нейронной сети набор обучающих данных;

2) определить основные средства для построения нейронной сети;

3) используя существующие примеры построения нейронных сетей, определить структуру такой сети и методы ее обучения.

## Методика и контрольный пример построения глубокой нейронной сети

Для построения глубокой нейронной сети с целью обнаружения угроз безопасности информации прежде всего требуется большой набор обучающих данных и специальные инструменты.

В данной работе предлагается обнаруживать угрозы исходя из анализа проходящего трафика по сети. С этой целью в качестве обучающих данных предлагается использовать набор NSL-KDD Data-Subsets, в котором содержатся уже размеченные данные с трафиком и специально проведенными в ходе его сбора атаками. В качестве примера возможных атак в трафике можно привести nmap-сканирование, backdoor, rootkit, guess_password, различные виды червей – worm, атаки на веб-сервисы, развернутые на apache2, и еще 32 возможные угрозы. Размер набора трафика: 4 898 431 запись.

Структура программы для обнаружения угроз безопасности информации включает в себя 4 основных файла:

1. Prepatation.py – преобразование первичных данных из набора в необходимые для подачи в нейронную сеть.
2. Neural_network.py – инициализация нейронной сети по структуре (Рисунок 2).
3. Train_model.py – обучение модели нейронной сети.
4. Analysis.py – получение результатов обучения.

| Цель | Используемое средство |
|---|---|
| Обучающий набор данных | NSL-KDD Data-Subsets 2012 |
| Написание основного кода программы | Pyton 3.9.0 64-bit |
| Подготовка обучающего набора данных | Библиотеки pandas, numpy |
| Построение нейронной сети | Библиотеки keras, tensorflow |
| Обучение нейронной сети | Библиотеки sklearn, matplotlib |
| Анализ обученной нейронной сети | Библиотеки sklearn, keras, numpy |
| Среда разработки | Visual Studio Code 1.68.1 |
| Вспомогательные библиотеки | os, asyncio, torch, seaborn, statistics |

Рисунок 1 – Используемые в работе средства
Figure 1 – Tools used in the operation

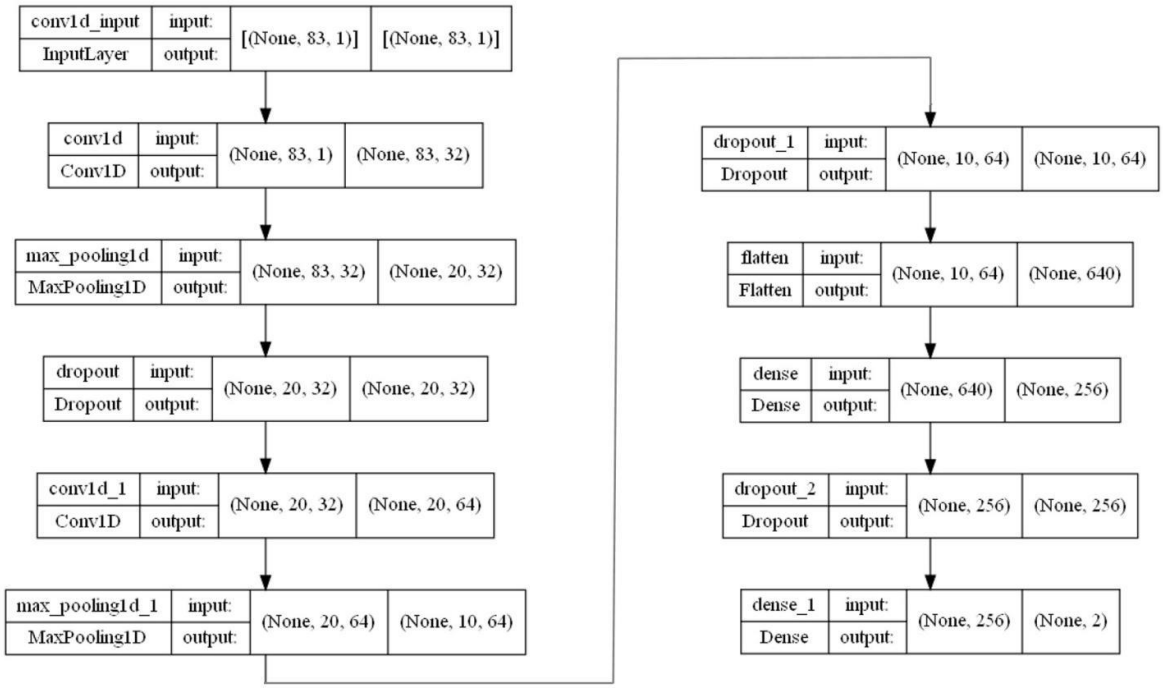


Рисунок 2 – Структура нейронной сети
Figure 2 – Neural network structure

Контрольный пример программы выложен в качестве репозитория [12]. Обучение нейронной сети проходит по методу «обучения с учителем» с использованием алгоритма стохастического градиентного спуска, основанного на адаптивной оценке моментов первого и второго порядка. Для вычисления потерь используется функция categorical_crossentropy, которая вычисляет категориальную потерю кроссентропии. В качестве входных данных нейронная сеть получает набор подготовленных данных и дискретную оценку каждой строки этих данных (Рисунок 3).

| | index | protocol | *** | difficult |
|---|---|---|---|---|
| 0 | 0 | tcp | *** | 2 |
| 1 | 1 | udp | *** | 1 |
| 2 | 2 | icmp | *** | 0 |
| 3 | 3 | udp | *** | 0 |
| 4 | 4 | icmp | *** | 2 |
| *** | *** | *** | *** | *** |
| *** | *** | *** | *** | *** |
| *** | *** | *** | *** | *** |
| *** | *** | *** | *** | *** |
| *** | *** | *** | *** | *** |
| 125789 | 125789 | tcp | *** | 0 |
| 125790 | 125790 | udp | *** | 1 |
| 125791 | 125791 | icmp | *** | 2 |
| 125792 | 125792 | udp | *** | 0 |
| 125793 | 125793 | icmp | *** | 1 |

| | index | 0 | 1 |
|---|---|---|---|
| 0 | *** | 1 | 0 |
| 1 | *** | 0 | 1 |
| 2 | *** | 0 | 1 |
| 3 | *** | 1 | 0 |
| 4 | *** | 1 | 0 |
| *** | *** | *** | *** |
| *** | *** | *** | *** |
| *** | *** | *** | *** |
| *** | *** | *** | *** |
| *** | *** | *** | *** |
| 125789 | *** | 1 | 0 |
| 125790 | *** | 0 | 1 |
| 125791 | *** | 1 | 0 |
| 125792 | *** | 0 | 1 |
| 125793 | *** | 1 | 0 |

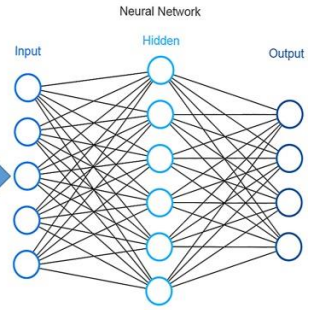


Рисунок 3 – Входные данные
Figure 3 – Input data

По результатам обучения были получены следующие характеристики:

1. F-оценка: 80.2 %.
2. Способность отличать класс (precision): 88.2 %.
3. Обнаружение определенного класса (recall): 73.4 %.
4. Доля правильных ответов (accuracy): 70.3 %.

Из представленных данных видно, что нейронная сеть позволяет по прошествии 100 эпох обучения показывать высокий показатель правильно распознанных угроз в сетевом трафике (~70 %). Из этого следует, что использование такой нейронной сети на достаточно высокой скорости обработки позволит пренебречь ошибками. К тому же данная программа является наглядным примером способности нейронной сети к обнаружению угроз нарушения безопасности, и если удастся со временем собрать больший банк данных трафика с угрозами и увеличить время обучения, например, до 1000 эпох и более, то показатель 70 % будет стремиться вверх.

Для упрощения процесса разработки и в качестве наглядной картины предлагается методика-алгоритм жизненного цикла нейронной сети (Рисунок 4). В данном алгоритме учтены лишь базовые основы написания программы без подробностей, но для наглядного представления функционирования нейронных сетей и правильной подготовки данных этого будет достаточно. Кроме того, в алгоритме приведены популярные наборы готовых данных для обучения и тестирования нейронных сетей в сфере информационной безопасности. Несмотря на большое количество готовых наборов данных для обучения, все они требуют предварительной подготовки для подачи их в нейронную сеть, что является одним из самых сложных процессов в написании кода программы с нейронными сетями. Точность и эффективность нейронной сети будет напрямую зависеть от качества предоставленных ей на вход данных, поэтому наилучшим вариантом будет сбор собственных данных для обучения. При этом возможно сразу учесть в каком виде будут выглядеть собранные данные и какие данные необходимо собирать исходя из прикладного применения нейронной сети. Для сбора данных в конкретном случае могут быть использованы следующие программы: Wireshark, Paessler PRTG, nProbe, tcpdump, The Dude и другие.

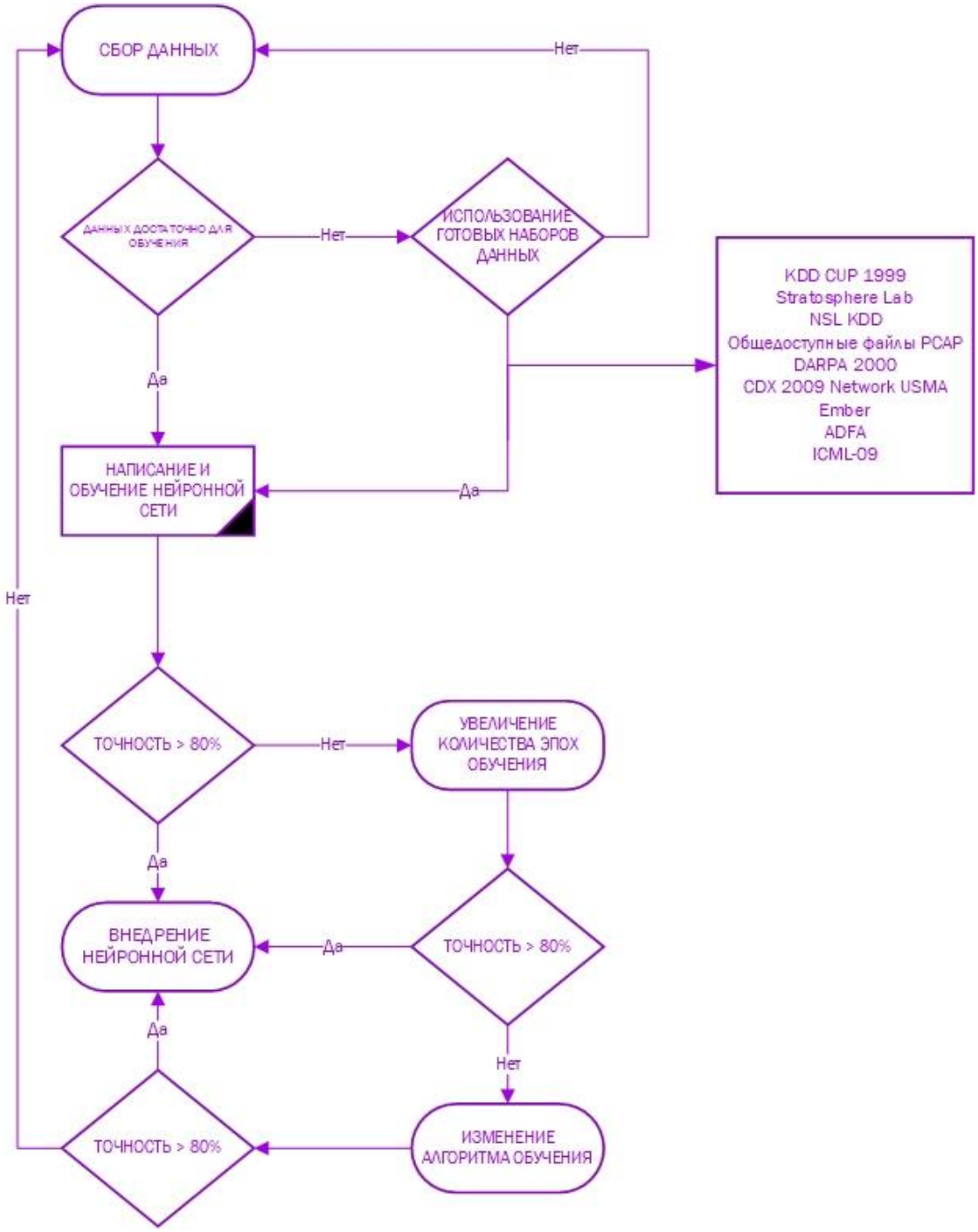


Рисунок 4 – Методика-алгоритм обучения нейронной сети
Figure 4 – Methodology-algorithm for neural network training

## Заключение

Таким образом, выявление угроз нарушения безопасности в компьютерных сетях возможно с использованием глубокой нейронной сети, пример реализации которой был представлен в данной работе. Для оптимизации контрольного примера необходимо подготовить больший набор данных для обучения и тренировки, а также внедрить данную нейронную сеть в систему обнаружения вторжений с возможностью дополнительного обучения. Несмотря на несовершенство реализации контрольного примера, результаты обнаружения и прогнозирования угроз нарушения безопасности в

компьютерных сетях являются достаточно высокими. Именно такая методика обнаружения угроз со временем будет одной из самых эффективных при противодействии компьютерным атакам и обеспечении информационной безопасности инфраструктуры компьютерной сети.

## СПИСОК ИСТОЧНИКОВ


1. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006, взамен ГОСТ Р 50922-96. 2008. 5 с. Доступно по: http://www.consultant.ru (дата обращения: 10.03.2022).
2. Демидов Р.А. Выявление угроз нарушения информационной безопасности в сетях с динамической топологией с использованием методов глубокого обучения. Диссертация на соискание ученной степени кандидата технических наук. 2018. 143 с.
3. *Нейронная сеть. Онлайн моделирование.* Доступно по: http://primat.org/demo/network/network.html#1 (дата обращения: 11.03.2022).
4. *Нейросети и глубокое обучение, глава 1: использование нейросетей для распознавания рукописных цифр.* Доступно по: https://habr.com/ru/post/456738/. (дата обращения: 13.03.2022).
5. Воробьев Л.В., Давыдов А.В., Щербина Л.П. *Системы и сети передачи информации: учебное пособие для студентов высших учебных заведений*. М.: Издательский центр «Академия»; 2009. 336 с.
6. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. *Сети связи: учебное пособие для студентов высших учебных заведений*. СПб.: БХВ Санкт-Петербург; 2010. 400 с.
7. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения: ГОСТ Р 52488-2005. 2007. 7 с. Доступно по: http://www.consultant.ru (дата обращения: 20.03.2022).
8. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем: ГОСТ Р 56546-2015. 2016. 17 с. Доступно по: http://www.consultant.ru (дата обращения: 20.03.2022).
9. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель: ГОСТ Р ИСО МЭК 15408-1-2012 взамен ГОСТ Р ИСО МЭК 15408-2008. 2013. 56 с. Доступно по: http://www.consultant.ru (дата обращения: 20.03.2022).
10. Крухмалев В.В., Гордиенко В.Н. *Основы построения телекоммуникационных систем и сетей: учебное пособие для студентов высших учебных заведений*. М.: Горячая линия-Телеком; 2004. 510 с.
11. Соколов А.В. Шаньгин В.Ф. *Защита информации в распределенных корпоративных сетях и системах*. Москва: ДМК; 2002. 656 с.
12. *Нейронная сеть для обнаружения угроз нарушения безопасности*. Доступно по: https://github.com/NikolaCloud/Neural.git (дата обращения: 17.05.2022).


## REFERENCES


1. Information protection. Basic terms and definitions: GOST R 50922-2006, instead of GOST R 50922-96. 2008. 5 p. Available by: http://www.consultant.ru (accessed on 10.03.2022). (In Russ.).
2. Demidov R.A. Identification of threats to information security violations in networks with dynamic topology using deep learning methods. Dissertation for the degree of Candidate of Technical Sciences. 2018. 143 p. (In Russ.).

3. *Neural network. Online modeling.* Available by: http://primat.org/demo/network/network.html#1 (accessed on 11.03.2022). (In Russ.).
4. *Neural networks and Deep Learning, Chapter 1: Using neural networks to recognize handwritten digits.* Available by: https://habr.com/ru/post/456738 (accessed on 13.03.2022). (In Russ.).
5. Vorobyev L.V. *Information transmission systems and networks: a textbook for students of higher educational institutions*. M.: Izdatel'skiy tsentr «Akademiya»; 2009. 336 p. (In Russ.).
6. Goldstein B.S. *Communication networks: a textbook for students of higher educational institutions.* SPb.: BKHV Sankt-Peterburg; 2010. 400 p. (In Russ.).
7. Information protection. Ensuring the security of telecommunication networks. General provisions: GOST R 52488-2005. 2007. 7 p. Available at: http://www.consultant.ru (accessed on 20.03.2022). (In Russ.).
8. Information protection. Vulnerabilities of information systems. Classification of information system vulnerabilities: GOST R 56546-2015. 2016:1-17. Available by: http://www.consultant.ru (accessed on 20.03.2022). (In Russ.).
9. Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technologies. Part 1. Introduction and general model: GOST R ISO IEC 15408-1-2012 instead of GOST R ISO IEC 15408-2008. 2013. 56 p. Available by: http://www.consultant.ru (accessed on 20.03.2022). (In Russ.).
10. Krukhmalev V.V., Gordienko V.N. *Fundamentals of building telecommunication systems and networks: a textbook for students of higher educational institutions*. 2004. 510 p. (In Russ.).
11. Sokolov A.V. *Information protection in distributed corporate networks and systems*. 2002. 656 p. (In Russ.).
12. *Neural network for detecting security threats*. Available by: https://github.com/NikolaCloud/Neural.git (accessed on 17.05.2022). (In Russ.).

## ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

**Клюев Станислав Геннадьевич**, кандидат технических наук, доцент Краснодарского высшего военного училища, Краснодар, Российская Федерация.
*e-mail:* s.g.klyuev@mail.ru
ORCID: 0000-0002-0534-9143

**Stanislav Gennadievich Klyuev**, Candidate of Technical Sciences, Associate Professor at Krasnodar Higher Military School, Krasnodar, Russian Federation.

**Трунов Евгений Евгеньевич**, курсант Краснодарского высшего военного училища, Краснодар, Российская Федерация.
*e-mail:* ittehnology2018@gmail.com
ORCID: 0000-0002-2623-9955

**Evgeny Evgenievich Trunov**, Cadet, Krasnodar Higher Military School, Krasnodar, Russian Federation.

*Статья поступила в редакцию 09.07.2022; одобрена после рецензирования 24.08.2022; принята к публикации 15.09.2022.*

*The article was submitted 09.07.2022; approved after reviewing 24.08.2022; accepted for publication 15.09.2022.*