DOI 10.36622/1682-7813.2024.27.4.003
УДК 349:004.056

НЕЙРОСЕТЕВОЙ СЕРВИС РЕГЛАМЕНТАЦИИ МЕР ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ (ЧАСТЬ III)

Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, С.В. Безбородых, А.Г. Остапенко, Н.П. Жуков

Рассматривается нейросетевая реализация модуля обнаружения и идентификации кибератак. В связи с этим предлагается методическое обеспечение для модуля, включая: обоснование применения нейронных сетей для анализа сетевого трафика; архитектуру модуля; базы данных для обучения нейросетевого модуля; разработку архитектуры используемой нейронной сети, взаимодействие с модулем регламентации мер противодействия; подготовку базы данных к машинному обучению. Используются аналоги и осуществляется целеполагание, включая постановку задач проекта. Оцениваются актуальность и перспектива использования результатов. Приводятся сравнительные оценки точности нейросетевых выводов. Методическое обеспечение имеет потенциал к совершенствованию, заключающийся в подборе формата преобразования трафика, более полно описывающим его активность, и в разработке архитектуры нейронной сети, позволяющей более точно проводить классификацию сетевого трафика.

Ключевые слова: нейросеть, модуль, кибератака, трафик, архитектура, база данных, машинное обучение.

Введение

Нейросетевые технологии обрели стремительное развитие, благодаря возросшим вычислительным мощностям, что открывает большие перспективы для их применения в сфере информационной безопасности. В этом контексте представляется актуальным данное исследование, посвященное разработке нейросетевого модуля обнаружения и идентификации кибератак, согласно классификатору CAPEC. Комплексность современных атак привела к эксплуатации нескольких типов уязвимостей, которые традиционные средства обнаружения вторжений не способны идентифицировать. Применение инструментов машинного обучения позволит провести вероятностную классификацию трафика, на основании чего возможно осуществить идентификацию различных пар атак и уязвимостей. На данный момент разработано несколько систем, в которых применяются алгоритмы машинного обучения. К их числу относятся:

- ViPNetIDSNS [1];
- PT Network Attack Discovery [2];
- Cisco Secure Endpoint [3];
- McAfee Endpoint Security [4].

Исследование вышеуказанных аналогов позволяет сделать вывод о наличии следующих противоречий между:

1. Объективной необходимостью в методическом обеспечении по формированию обучающих баз данных и в алгоритмическом обеспечении по разработке архитектуры нейронной сети для эффективной классификации сетевого трафика и отсутствием таковых у приведенных аналогов;
2. Объективной необходимостью в идентификации кибератак согласно классификаторам угроз информационной безопасности и отсутствием данного функционала у выявленных аналогов, которые используют алгоритмы машинного обучения для обнаружения аномалий в активности сетевого трафика.

Отсюда в качестве предмета исследования выступают технические решения нейросетевой реализации модуля для обнаружения и идентификации кибератак на основе анализа активности сетевого трафика.

Предлагаемое техническое решение описывает архитектуру нейронной сети, формат представления сетевого трафика и

формирование обучающей базы данных, на основании которых возможно реализовать модуль, способный к идентификации сетевых атак и их уязвимостей в соответствии с классификатором.

1 Обоснование применения нейронных сетей для анализа сетевого трафика

Реализация кибератаки влияет на поведение сети, так как злоумышленники эксплуатируют те же протоколы обмена данными, что и обычные устройства. Множество систем анализа трафика (Network Traffic Analysis, NTA) и сетевых систем обнаружения вторжения (Network Intrusion Detection System, NIDS) показывают, что по анализу сетевого трафика возможно обнаружить его аномальную активность, что может свидетельствовать о реализации атаки. Большинство данных систем работает сигнатурным методом, поэтому при условии, что известна сигнатура кибератаки, её можно однозначно идентифицировать [6,7].

Для разработки сигнатур необходимо вручную анализировать вредоносный сетевой трафик, выделять из него общие признаки и на их основании составлять набор правил, по которым можно обнаружить вредоносную активность. Но существуют алгоритмы машинного обучения, позволяющие автоматизировать данный процесс. Основываясь на обучающих базах данных, они могут самостоятельно выделить ключевые признаки, свидетельствующие о реализации сетевой атаки. Необходимо подобрать такой метод машинного обучения, который способен идентифицировать сетевые атаки согласно классификатору CAPEC.

Такие методы машинного обучения подразделяются на два вида: обучение с учителем [7] и без него [8]. К основным задачам машинного обучения без учителя относятся [8]: кластеризация, поиск ассоциаций, поиск аномалий, уменьшение размерности

Использование данных алгоритмов позволило бы провести автоматическую кластеризацию сетевого трафика на нормальный и аномальный, а также, если известно общее количество атак в обучающем наборе данных, можно провести кластеризацию трафика по каждой из них. Поиск ассоциаций позволит установить, чем данные одного кластера отличаются от данных другого. Если будет получен трафик, значительно отличающийся от обучающего, то это может свидетельствовать о реализации какой-либо новой сетевой атаки. Также в базах данных нередко попадаются коррелирующие характеристики, которые нет смысла отдельно обрабатывать, поэтому для уменьшения времени вычислений стоит их объединить, в чем также может помочь машинное обучение без учителя.

Машинное обучение без учителя обладает многими плюсами, но они не подходят для решения поставленной задачи. Алгоритмы могут провести самостоятельную кластеризацию, но нет возможности проконтролировать этот процесс. Ошибка может привести к неправильной работе, что обусловит большое количество ложно положительных и ложно отрицательных ответов. Для предотвращения подобных ситуаций требуется проводить тестирование на базах данных, в которых известен правильный ответ, что нивелирует преимущество алгоритмов без учителя над алгоритмами с учителем. Алгоритмы без учителя являются более подходящими для первичного анализа баз данных, которые впоследствии будут использованы для машинного обучения с учителем.

Наиболее перспективным применением данных алгоритмов представляется поиск аномалий. Если провести обучение на базах данных, содержащих исключительно нормальный сетевой трафик, любое отклонение от него будет означать вредоносную активность.

Анализ сетевого трафика представляет собой задачу классификации, ибо необходимо обработать поступающий трафик и определить, к какому классу атак он относится. Алгоритмы машинного обучения соответствуют данным требованиям, так как одним из распространённых их применений является решение задача много классовой классификации. Существует множество алгоритмов, способных решать данную задачу, но наиболее гибким и способным к построению сложных математических моделей является применение искусственных нейронных сетей.

Изначально нейронные сети предназначались для решения задач регрессии, то есть предсказания числа. Но оказалось, что их можно адаптировать для классификации данных, если изменить количество выходных нейронов и применить правильные функции активации и потерь.

Нейронные сети представляют собой граф, состоящий из вершин, называемых нейронами. Нейроны подразделяются на входные и выходные. Задачей нейросетей является расчет значений на выходных нейронах, основываясь на полученных данных на входных нейронах. Функции, по которым рассчитываются значения, представляют математическую модель, которая должна соответствовать модели обучающих данных, чтобы выходные значения всегда оказывались верны.

Нейронные сети показали свою эффективность в решениях задач классификации, во многом благодаря способности к глубокому обучению.

Применение нейронных сетей при анализе сетевого трафика позволит идентифицировать сетевые атаки согласно классификатору CAPEC, при условии, что будут доступны промаркированные соответствующим образом базы данных.

2 Архитектура модуля обнаружения и идентификации кибератак

Архитектура нейросетевого модуля представляет собой систему, состоящую из сенсора и сервера, обрабатывающем сетевой трафик. Она изображена на рис. 1.

Рис. 1. Архитектура нейросетевого модуля обнаружения и идентификации кибератак

Сенсор занимается перехватом поступающего из вне сетевого трафика и преобразует его во формат flow-протокола NetFlow. Он объединяет сетевые пакеты, участвовавшие в сеансе связи между устройствами, в один поток и извлекает характеристики о его активности. Они представлены количественно, поэтому их очень удобно и легко применять в машинном обучении. NetFlow был разработан компанией Cisco в середине 1990 годов как проприетарный протокол и предназначался для развертывания только на устройствах Cisco, но некоторые устройства сторонних производителей также получили его поддержку. Многие другие протоколы являются аналогами NetFlow. Netflow v9 – его последняя версия на данный момент извлекает 79 характеристик из активности сетевого трафика.

На сервере развернут нейросетевой модуль, принимающий данные об активности сетевого трафика с сенсора и подвергающий их анализу. Для удобства пользователя был разработан графический интерфейс, позволяющий выбрать файл для анализа. Если обнаружена атака, то на экран будет выведено сообщение и автоматически отправлено модулю регламентации мер противодействия. Также для обеспечения возможности дообучения модели сервер имеет доступ к базе данных, содержащей вредоносный сетевой трафик.

3 Базы данных для обучения нейросетевого модуля

На данный момент существует множество общедоступных баз данных, содержащих данные о вредоносном сетевом трафике, которые можно использовать для машинного обучения.

Наиболее актуальными на сегодняшний день являются следующие базы данных:

– UNSW-NB15;
– BoT-IoT;
– ToN-IoT;
– CSE-CIC-IDS2018.

База данных UNSW-NB15 была выпущена в 2015 году университетом Нового Южного Уэльса в Австралии. Она содержит данные о сетевом трафике, представленном 49 признаками, а также 10 различными классами, представленными в табл. 1.

Таблица 1

Количество записей для тренировочной и тестовой выборки каждого класса базы данных UNSW-NB15

Класс атак	**Количество записей**
Normal	93000
Analysis	2677
Backdoor	2329
DoS	16353
Exploits	44525
Fuzzers	24246
Generic	58871
Reconnaissance	13987
Shellcode	1511
Worms	174
Общее количество записей	257673

База данных BoT-IoT была разработана тем же университетом, что и UNSW- NB15. Она включает 43 характеристики и так же 10 классов атак, представленных в табл. 2.

Таблица 2

Количество записей для тренировочной и тестовой выборки каждого класса базы данных BoT-IoT

Класс атак	**Подкласс атак**	**Количество записей**
BENIGN	BENIGN	9543
Information gathering	Service scanning	1,463,364
	OS Fingerprinting	358,275
DDoS attack	DDoS TCP	19,547,603
	DDoS UDP	18,965,106
	DDoS HTTP	19,771

Продолжение табл. 2

Класс атак	Подкласс атак	Количество записей
DoS attack	DoS TCP	12,315,997
	DoS UDP	20,659,491
	DoS HTTP	29,706
Information theft	Keylogging	1469
	Data theft	118
Общее количество записей		73,370,443

База данных ToN-IoT содержит сетевой трафик, сгенерированный интернетом вещей. В неё входят данные, собранные с различных операционных систем Windows 7, Windows 10, Ubuntu 14 и Ubuntu 18 TLS. Классы атак, содержащиеся в ToN-IoT представлены в табл. 3.

Таблица 3

Количество записей для каждого класса атак базы данных ToN-IoT

Класс атак	Количество записей
DoS	20,000
DDoS	20,000
Scanning	20,000
Ransomware	20,000
Backdoor	20,000
Injection	20,000
Cross-Site Scripting (XSS)	20,000
Password	20,000
Man-In-The-Middle (MITM)	1043
Общее количество записей	161043

База данных CIC-IDS-2018 была выпущена в 2018 году. Для анализа сетевой активности применялся анализатор CICFlowMeter. Всего в ней содержится 7 классов атак, представленных в табл. 4.

Таблица 4

Количество записей для каждого класса атак базы данных CIC-IDS-2018

Классы атак	Количество записей
FTP-BruteForce	193360
SSH-BruteForce	187589
DoS attacks-GoldenEye	41508
Dos attacks-Slowloris	10990
DoS attacks-Hulk	461912
Dos attacks-SlowHTTPTest	139890

Продолжение табл. 4

Классы атак	Количество записей
DDoS attacks-LOIC-HTTP	576191
DDOS attack-HOIC	686012
DDOS attack-LOIC-UDP	1730
Brute Force – Web	611
Brute Force – XSS	230
SQL Injection	117
Infiltration	161934
Bot	286191
Benign	13484708
Общее количество записей	16 232 973

Все перечисленные базы данных можно использовать для обучения нейронной сети. Однако, данные в них представлены разным образом. У баз данных отличаются количества характеристик и реализованные атаки. В CIC-IDS-2018 используется программа CICFlowMeter для анализа сетевого трафика, в отличие от BoT-IoT и UNSW-NB15, в которых используются Argus и Zeek (Bro). Поэтому обучение сразу на всех четырех базах данных не представляется возможным. Данные, собранные в разнобой, внесут путаницу и приведут к неверному обучению нейронной сети. Необходимо, чтобы данные были представлены в едином формате. Поэтому в качестве основной базы данных была выбрана NF-UQ-NIDS-v2, объединяющая в себе четыре предыдущие базы данных. Она обладает 45 характеристиками и 21 различными классами атак, представленными в табл. 5.

Таблица 5

Количество записей каждого класса атак базы данных NF-UQ-NIDS-v2

Класс атак	Количество записей
Benign	25165295
DDoS	21748351
Reconnaissance	2633778
Injection	684897

Продолжение табл. 5

DoS	17875585
Brute Force	123982
Password	1153323
XSS	2455020
Infilteration	116361
Exploits	31551
Scanning	3781419
Fuzzers	22310
Backdoor	18978
Bot	143097
Generic	16560
Analysis	2299
Theft	2431
Shellcode	1427
MITM	7723
Worms	164
Ransomware	3425

К сожалению, данная база данных не адаптирована под классификатор CAPEC, и имеющиеся классы представляют собой не идентификатор, а наименование общей разновидности атак. У некоторых из них дано подробное описание, включающее в себя набор утилит, с помощью которых данная атака реализовывалась. Благодаря этому возможно подобрать идентификаторы CAPEC, которые могли бы соответствовать рассматриваемой атаке. Результат полученных соответствий представлен в табл. 6.

Таблица 6

Список реализованных атак базы данных NF-UQ-NIDS-v2 [9]

Класс	**Описание**	**ПО**	**Идентификатор CAPEC**
Benign	Нормальный не вредоносный трафик	-	-
DDoS	Атака, аналогичная DoS, но имеющая несколько различных распределенных источников	LOIC, HOIC	CAPEC-486: UDP Flood CAPEC – 488: HTTP Flood CAPEC – 482: TCP Flood
Reconnaissance	Цель атаки – найти данные об инфраструктуре сети, включая сетевые службы и активные устройства. Может быть достигнута с помощью сканирования сетевых портов и анализа пакетов.	-	CAPEC – 285: ICMP Echo Request Ping CAPEC – 297: TCP ACK Ping CAPEC – 298: UDP Ping CAPEC – 287: TCP SYN Scan CAPEC – 301: TCP Connect Scan CAPEC – 308: UDP Scan CAPEC – 300: Port scanning CAPEC – 292: Host discovery
Injection	Атаки, предоставляющие ненадежные входные данные и направленные на изменение выполнения кода	-	CAPEC – 66: SQL Injection
DoS	Попытка перегрузки ресурсов компьютерной системы с целью нарушения ее доступности	Hulk, SlowHTTPTest, GoldenEye, Slowloris	CAPEC – 469: HTTP DoS
Brute Force	Атака, направленная на получение логинов и паролей учетных записей	Patator	CAPEC-49: Password Brute Forcing

Продолжение табл. 6

Класс	**Описание**	**ПО**	**Идентификатор CAPEC**
Password	Различные атаки, направленные на получение паролей с помощью грубой силы или перехвата	Hydra, cewl	CAPEC-16: Dictionary-based Password Attack CAPEC-55: Rainbow Table Password Cracking CAPEC-70: Try Common or Default Usernames and Passwords
XSS	Атака внедрения, при которой злоумышленник использует веб-приложения для отправки вредоносных скриптов конечным пользователям	XSSer	CAPEC – 588: DOM-Based XSS CAPEC – 591: Reflected XSS CAPEC – 592: Stored XSS
Infilteration	Атака, при которой вредоносный файл отправляется по электронной почте. Далее следует бэкдор, который сканирует сеть на наличие других уязвимостей	-	CAPEC-98: Phishing
Exploits	Атака представляют собой последовательности команд, управляющих поведением хоста с помощью известной уязвимости	-	-
Scanning	Атака, состоящая из множества методов, направленных на получение информации о сетях и хостах, также известна как зондирование	Nessus, Nmap	CAPEC – 285: ICMP Echo Request Ping CAPEC – 297: TCP ACK Ping CAPEC – 298: UDP Ping CAPEC – 287: TCP SYN Scan CAPEC – 301: TCP Connect Scan CAPEC – 308: UDP Scan CAPEC – 300: Port scanning
Fuzzers	Атака, при которой злоумышленник отправляет большие объемы случайных данных, которые приводят к сбою системы	-	CAPEC-28: Fuzzing

Продолжение табл. 6

Класс	**Описание**	**ПО**	**Идентификатор CAPEC**
Backdoor	Метод, направленный на обход механизмов безопасности путем ответа на запросы специально созданных клиентских приложений	Metasploit	-
Bot	Атака, которая позволяет злоумышленнику удаленно управлять несколькими захваченными компьютерами для выполнения вредоносных действий	Zeus, Ares	CAPEC-648: Collect Data from Screen Capture CAPEC-568: Capture Credentials via Keylogger
Generic	Атака, вызывающая коллизию с каждым блочным криптографическим шифром	-	-
Analysis	Группа, включающая в себя различные атаки на поиск портов и вредоносное ПО	-	CAPEC – 300: Port scanning
Theft	Группа атак, направленных на получение конфиденциальных данных через регистрирование нажатий клавиш	-	CAPEC-568: Capture Credentials via Keylogger
Shellcode	Вредоносная программа, проникающая в код для управления хостом жертвы	-	CAPEC-242: Code Injection
MITM	"Человек посередине" - атака, которая помещает злоумышленника между жертвой и хостом, с которым жертва пытается установить связь, с целью перехвата трафика и коммуникаций	Ettercap	CAPEC-94: Adversary in the Middle (AiTM)
Worms	Атаки, которые самостоятельно повторяются и распространяются на другие компьютеры	-	-

Окончание табл. 6

Класс	**Описание**	**ПО**	**Идентификатор CAPEC**
Ransomware	Атака, которая шифрует файлы, хранящиеся на хосте, и запрашивает компенсацию в обмен на расшифровщик	Metasploit	CAPEC-92: Forced Integer Overflow CAPEC-100: Overflow Buffers CAPEC-30: Hijacking a Privileged Thread of Execution

Нейронная сеть, обученная на базе данных NF-UQ-NIDS-v2, не сможет однозначно установить идентификатор CAPEC у обнаруженной атаки, а лишь установит область возможных идентификаторов, которые могут ей соответствовать. Для решения данной проблемы была сформирована собственная база данных, путем реализации сетевых атак, перехвата сетевого трафика и преобразования его в формат NetFlow. Полученные данные промаркированы согласно классификатору CAPEC и обладают структурой, представленной в табл. 7.

Таблица 7

Структура данных нейросети

Номер записи	**Характеристики сетевого потока**				**Метка атаки**
	Номер протокола	**Количество переданных пакетов**	**…**	**Продолжительность сессии, мс**	
…	…	…	…	…	…
Момент реализации атаки	n	m	…	k	Идентификатор CAPEC
…	…	…	…	…	…

На их основании возможно провести машинное обучение нейронной сети, способную к классификации сетевого трафика, где в качестве класса выступает идентификатор CAPEC.

Заключение

Предложены форматы преобразования сетевого трафика и формирования обучающей базы данных, на основании которых возможно реализовать модуль, способный к идентификации сетевых атак и их уязвимостей в соответствии с классификатором CAPEC.

Предложенный подход описывает архитектуру нейронной сети, формат представления сетевого трафика и формирование обучающей базы данных, на основании которых возможно реализовать модуль, способный к идентификации сетевых атак и их уязвимостей в соответствии с классификатором.

Методическое обеспечение можно использовать в информационных системах для реализации системы перехвата вредоносного сетевого трафика и формирования на его основе баз данных, пригодных для машинного обучения;

алгоритмическое обеспечение, описывающее архитектуру нейронной сети, позволяет реализовать модуль по обнаружению и идентификации кибератак.

Сформированное методическое обеспечение возможно использовать для формирования собственной базы данных, содержащей промаркированные записи, где в качестве метки выступают идентификаторы CAPEC, которое пригодно для машинного обучения и позволяет обеспечить высокую точность результата обученной нейронной сети.

Методическое и алгоритмическое обеспечение имеет потенциал к совершенствованию, заключающийся в подборе формата преобразования трафика, более полно описывающем его активность, и в разработке архитектуры нейронной сети, позволяющей более точно проводить классификацию сетевого трафика.

Список литературы

1. Система обнаружения компьютерных атак ViPNetIDSNS//Infotecs URL: https://infotecs.ru/products/vipnet-ids-ns/ (дата обращения 16.06.2024).

2. Обзор PT Network Attack Discovery // Positive Technologies URL: https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/#scenarios (дата обращения16.06.2024).

3. Cisco Secure Endpoint // Cisco URL: https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html (дата обращения 16.06.2024).

4. EndPoint Security McAfee:Products, Capabilities and Features // Cynet URL: https://www.cynet.com/endpoint-security/endpoint-security-mcafee-products-capabilities-and-features/ (дата обращения 16.06.2024).

5. Suricata URL: https://suricata.io (дата обращения 16.06.2024).

6. Что такое системы анализа трафика (Network Traffic Analysis, NTA), их отличие от NDR и IDS // Security Vision URL: https://www.securityvision.ru/blog/chto-takoe-sistemy-analiza-trafika-network-traffic-analysis-nta-ikh-otlichie-ot-ndr-i-ids/ (дата обращения: 16.06.2024).

8. Jordan, M. I.; Mitchell, T. M. (17 July 2015). "Machine learning: Trends, perspectives, and prospects". Science. 349 (6245): 255–260.

9. Machine Learning-Based NIDS Datasets // URL: https://staff.itee.uq.edu.au/marius/NIDS_datasets/#RA5 (дата обращения 10.06.2024).

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 17.07.2024

Информация об авторах

Григорий Александрович Остапенко – д-р техн. наук, профессор, Финансовый университет при Правительстве Российской Федерации, e-mail: ost@fa.ru

Алексей Павлович Васильченко – аспирант, Финансовый университет при Правительстве Российской Федерации, e-mail: rainichek@yandex.ru

Александр Алексеевич Остапенко – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

Станислав Витальевич Безбородых – студент, Воронежский государственный технический университет, e-mail: stanislav.bezb@mail.ru

Остапенко Александр Григорьевич – д-р техн. наук, профессор, заведующий кафедрой, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Жуков Никита Павлович – студент, Воронежский государственный технический университет, e-mail: znp8b00ff.gmail.com

NEURAL NETWORK SERVICE FOR REGULATING MEASURES TO COUNTER CYBERATTACKS (PART III)

G.A. Ostapenko, A.P. Vasilchenko, A.A. Ostapenko, S.V. Bezborodykh, A.G. Ostapenko, N.P. Zhukov

The neural network implementation of the cyberattack detection and identification module is considered. In this regard, methodological support for the module is proposed, including: justification of the use of neural networks for analyzing network traffic; architecture of the module; databases for training the neural network module; development of the architecture of the neural network used, interaction with the module for regulating countermeasures; preparation of the database for machine learning. Analogues are used and goal-setting is carried out, including setting the objectives of the project. The relevance and prospects of using the results are evaluated. Comparative estimates of the accuracy of neural network conclusions are given. Methodological support has the potential for improvement, consisting in the selection of a traffic conversion format that more fully describes its activity, and in the development of a neural network architecture that allows for more accurate classification of network traffic.

Keywords: neural network, module, cyberattack, traffic, architecture, database, machine learning.

Submitted 17.07.2024

Information about authors

Gregory A. Ostapenko – Dr. Sc. (Technical), Professor, Financial University under the Government of the Russian Federation, e-mail: ost@fa.ru

Alexey P. Vasilchenko – graduate student, Financial University under the Government of the Russian Federation, e-mail: rainichek@yandex.ru

Alexandr A. Ostapenko – graduate student, Voronezh State Technical University, e-mail: alexostap123@gmail.com

Stanislav V. Bezborodykh – student, Voronezh State Technical University, e-mail: sfrvvv@yandex.ru

Alexandr G. Ostapenko – Dr. Sc. (Technical), Professor, Head of the Department, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Nikita P. Zhukov – student, Voronezh State Technical University, e-mail: znp8b00ff.gmail.com