Обзорная статья
УДК 681.3; DOI: 10.61260/2307-7476-2024-2-39-46

К ВОПРОСУ ОБЕСПЕЧЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ

✉**Лабинский Александр Юрьевич.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***labynsciy@yandex.ru***

Аннотация. Рассмотрены:

– принципы и средства обеспечения безопасности корпоративной сети, а также особенности виртуальных частных сетей, обеспечивающих надежную защиту и защищенную передачу данных;

– принципы и меры обеспечения безопасности корпоративной сети, а также виды защиты информации, обеспечиваемые указанными мерами защиты;

– виртуальные частные сети (VPN), обеспечивающие безопасное зашифрованное подключение пользователя к сети. Использование VPN обеспечивает надежную защиту данных, маскировку геолокации пользователя, доступ к региональному контенту и защищенную передачу данных;

– системы выявления и предотвращения угроз взлома сети, среди которых основное внимание уделено пакету программ Kali Linux, а также особенности подсистемы Windows для Linux и средства сетевого мониторинга Windows;

– средства сетевого мониторинга Windows, среди которых утилиты, работающие в консольном режиме командной строки и позволяющие проверять доступность удаленных персональных компьютеров и диагностировать соединение.

Пакет программ Kali Linux – это дистрибутив для операционной системы Linux, который имеет более 600 предустановленных программ тестирования проникновения в сеть. Среди возможностей пакета в статье рассмотрены поиск и эксплуатация уязвимостей сети, проверка правильности настройки SSL-сертификата и открытых портов, трассировка маршрута передачи данных, проверка доступности серверов и поиск проблем сети.

Ключевые слова: вредоносная программа, защита информации, виртуальная частная сеть, пакет программ Kali Linux, средства сетевого мониторинга Windows, прокси-серверы, межсетевые экраны

Для цитирования: Лабинский А.Ю. К вопросу обеспечения сетевой безопасности // Природные и техногенные риски (физико-математические и прикладные аспекты). 2024. № 2 (50). С. 39–46. DOI: 10.61260/2307-7476-2024-2-39-46.

Review article

ON THE ISSUE OF NETWORK SECURITY

✉**Labinskiy Alexander Yu.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***labynsciy@yandex.ru***

Abstract. The following are considered:

– principles and means of ensuring the security of a corporate network, as well as features of virtual private networks that provide reliable protection and secure data transmission;

– principles and measures to ensure the security of the corporate network, as well as the types of information protection provided by these security measures;

– virtual private networks (VPNs) that provide a secure encrypted user connection to the network. Using a VPN provides reliable data protection, masking the user's geolocation, access to regional content and secure data transfer;

– systems for detecting and preventing network hacking threats, among which the main focus is on the Kali Linux software package, as well as features of the Windows subsystem for Linux and Windows network monitoring tools;

– Windows network monitoring tools, including utilities that work in console command-line mode and allow you to check the availability of remote personal computers and diagnose the connection.

The Kali Linux software package is a distribution package for the Linux operating system that has more than 600 preinstalled network penetration testing programs. Among the features of the package, the article discusses the search and exploitation of network vulnerabilities, checking the correct configuration of the SSL certificate and open ports, tracing the data transfer route, checking the availability of servers and searching for network problems.

Keywords: malware, information protection, virtual private network, Kali Linux software package, Windows network monitoring tools, proxy-servers, firewalls

For citation: Labinskiy A.Yu. On the issue of network security // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty) = Natural and man-made risks (physico-mathematical and applied aspects). 2024. № 2 (50). P. 39–46. DOI: 10.61260/2307-7476-2024-2-39-46.

Введение

Сетевая безопасность – это набор требований и политик, которые предъявляются к сетевой корпоративной инфраструктуре для анализа ее работы и недопущения доступа к данным злоумышленников, изменения этих данных, их модификации, а также отказа работы сети или ее отдельных ресурсов.

Для этой цели применяются аппаратные и программные средства и устройства, в том числе межсетевые экраны, антивирусные программы, средства мониторинга сети, средства обнаружения попыток несанкционированного доступа (вторжения), прокси-серверы и серверы аутентификации. Данные средства обеспечивают сетевую безопасность, контролируют входящий и исходящий интернет-трафик, контролируют сетевую активность приложений, защищают от хакеров и загрузки вредоносного программного обеспечения (ПО).

Сформулируем постановку задачи. Нужно рассмотреть подходы к решению задачи обеспечения сетевой безопасности. Тема статьи актуальна, так как в 2003 г. сетевые атаки по всему миру нанесли ущерб в 670 млн долл., а в 2021 г. ущерб от сетевых атак в 86 странах составил уже 6 трлн долл. Актуальность проблемы сетевой безопасности постоянно увеличивается, и средствам защиты информации посвящено много работ [1–11].

Обеспечение безопасности сети

Применительно к корпоративной сети можно выделить следующие основные принципы, позволяющие обеспечить безопасность:

– защита подключенных к сети устройств. Для надежной защиты подключенного к сети устройства следует использовать современные подходы к обеспечению безопасности. Для компьютеров, подключенных к сети, следует использовать антивирусное ПО, которое должно постоянно обновляться;

– нужно предусмотреть, чтобы сетевые устройства были стойкими к отказам и могли быстро восстанавливаться. Для этого необходимо следить за состоянием сетевых устройств, для чего выполнять систематический мониторинг инфраструктуры и при необходимости использовать средства защиты;

– в целях безопасности нужно непрерывно контролировать пропускную способность сети. Любая атака на сеть всегда влечет за собой большие затраты, в том числе на восстановление работоспособности системы. Поэтому возникает необходимость в разработке как методик защиты инфраструктуры, так и методик использования средств защиты от атак на сеть. Эти мероприятия обычно срывают замыслы вредителей сети и уменьшают расходы на сохранность данных;

– важно обеспечить устойчивость сети к отказам, а также предусмотреть возможность быстрого восстановления сети. Для этого нужно использовать дублирование критических ресурсов сети и обеспечивать их автоматическую замену.

Обычно инфраструктура сети может подвергаться как активным, так и пассивным атакам.

Атаки на сетевую инфраструктуру могут быть как активными, так и пассивными (в зависимости от вредоносного ПО, которое используют злоумышленники). Поэтому, чтобы обеспечить безопасность сети, используются комплексные меры, включающие в себя:

- виртуальные частные сети – VPN (Virtual Private Network);
- промежуточные серверы в качестве посредника между пользователями и целевыми серверами;
- системы обнаружения и защиты от взлома;
- средства обнаружения и защиты от атак на сеть;
- экраны между элементами сети;
- мониторинг сетевого трафика.

Указанные выше меры позволяют осуществить следующую защиту:

- защита элементов сети от атак на сеть;
- защита подключения внешних устройств к сети;
- защита ПО путем мониторинга и контроля его работы;
- защита сетевых банковских операций.

Виртуальные частные сети

VPN обеспечивают безопасное зашифрованное подключение пользователя к сети, с которым он может обходить локальные ограничения и сохранять конфиденциальность. Физическая частная сеть (группа компьютеров, образующих виртуальную сеть) не принадлежит пользователю. В такой сети может находиться ограниченный круг лиц. Данные защищаются от третьих лиц путем шифрования. Администрация VPN не пускает посторонних пользователей, проверяет источник трафика и следит, чтобы передаваемые данные не утекали за пределы сети в открытом виде. Подключение к VPN происходит с помощью специального приложения.

Когда пользователь заходит в сеть Интернет, его устройству присваивается уникальный IP-адрес. При подключении к сети через VPN оригинальный IP-адрес становится невиден. Вместо него отображается адрес виртуальной частной сети, что позволяет:

- обходить локальные ограничения (блокировки ресурсов сети Интернет);
- сохранять анонимность (подключение к сети Интернет шифруется).

VPN шифрует данные с помощью различных протоколов, например, протокола OpenVPN, который оптимален по набору характеристик (скорости, степени защиты и надежности).

Эксперты «Лаборатории Касперского» отмечают следующие преимущества использования VPN:

- надежная защита данных;
- маскировка геолокации;
- доступ к региональному контенту;
- защищенная передача данных.

Системы выявления и предотвращения угроз взлома сети

В настоящее время широкое распространение получил пакет программ Kali Linux, предназначенный для проведения тестов на безопасность компьютерной сети [10, 11]. Kali Linux имеет более 600 предустановленных программ тестирования проникновения в сеть.

Kali Linux – это дистрибутив для операционной системы (ОС) Linux. Одной из ключевых особенностей Kali Linux является огромное количество предустановленных утилит, необходимых для проведения разнообразных тестов на проникновение в сеть и аудита безопасности. Рассмотрим некоторые инструменты Kali Linux.

Поиск и эксплуатация уязвимостей. Программа WPScan служит для проверки сайтов, работающих на WordPress. Эта программа может определить старые версии WordPress, тему оформления, установленные плагины, показать известные уязвимости в плагинах и темах оформления WordPress.

Поиск уязвимости типа SQL-инъекция. С помощью программы SqlMap можно найти уязвимость типа SQL-инъекция. SQL-инъекция – это одна из самых серьёзных уязвимостей веб-приложений.

Сбор информации о сайте. Программа WhatWeb собирает информацию о применяемых на данном сайте технологиях, используемых при разработке сайта.

Сбор информации о Web-приложении. Программа Wig собирает и идентифицирует ряд систем управления контентом Web-приложения.

Проверка правильности настройки SSL-сертификата. Программа TestSsl осуществляет проверку правильности SSL-сертификата (использование уязвимых шрифтов и т.п.).

Проверка открытых портов. Программа Nmap осуществляет проверку портов. Для используемых служб порты должны быть открыты, а для неиспользуемых – закрыты.

Трассировка маршрута передачи данных. Трассировка выполняется программой TraceRoute. Трассировка маршрута пакета до сетевого хоста показывает все промежуточные узлы, через которые проходит пакет, пока доберётся до адресата. Трассировка может применяться для выявления связанных с работой компьютерной сети проблем, а также для исследования сети (определения структуры сети, поиска промежуточных сетевых узлов).

Проверка доступности серверов и поиска проблем сети. Программа Ping отправляет на указанный хост запрос и показывает время ответа (если ответ пришёл). В случае возникновения ошибки, программа ping выводит код ошибки. Такое поведение позволяет проверить, есть ли доступ до определённого хоста, а также выявить некоторые проблемы сети, такие как потеря пакетов и большие задержки.

Популярные приложения дистрибутива Kali Linux:

- John the Ripper – взлом паролей методом перебора;
- Aircrack-ng – тестирование безопасности Wi-Fi сетей;
- THC Hydra – еще один инструмент для взлома аутентификации;
- Burb Suite – поиск уязвимостей на сайтах и в веб-приложениях;
- Wireshark – анализатор сетевых пакетов.

Дистрибутив Kali Linux основан на дистрибутиве ОС Linux Ubuntu (Debian) и распространяется свободно, без покупки лицензий. Поддерживает практически все известные файловые системы, типы накопителей, интерфейсы. Первая версия дистрибутива Kali Linux (версия 1.0) вышла в марте 2013 г., а последняя (версия 2021.4) – в декабре 2021 г.

Подсистема Windows для Linux

Подсистема Windows Subsystem for Linux (WSL) является уровнем ПО, используемым для запуска Linux-приложений, представляющих собой двоичные исполняемые файлы в формате ELF, в ОС Windows 10.

В сравнении с системами, использующими полную виртуализацию, подсистема WSL требует меньше ресурсов. Поэтому подсистема WSL наиболее часто используется для запуска многих Linux-приложений на ОС Windows.

Схема взаимодействия подсистемы WSL и Windows представлена на рис. 1.

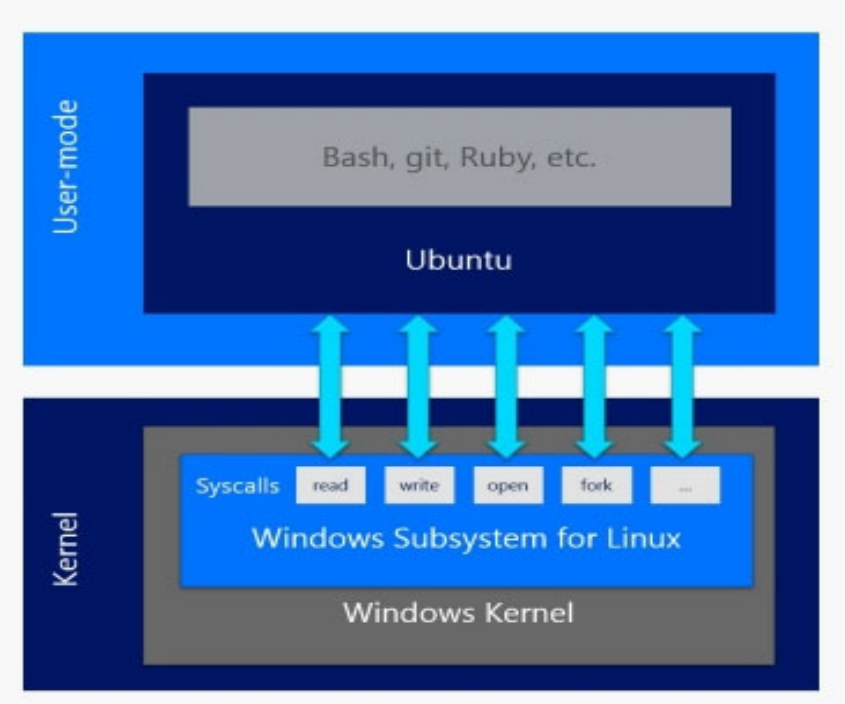

Рис. 1. **Схема взаимодействия подсистемы WSL и Windows**

Запущенные через WSL приложения Windows и Linux имеют доступ ко всем файлам пользователя. Подсистема WSL предназначена только для 64-битных редакций Windows 10, а также может быть активирована на более поздних версиях Windows 10, включая Anniversary Update. По заявлениям корпорации Microsoft, подсистема WSL может использоваться как инструмент для разработчиков, веб-разработчиков и пользователей, работающих с приложениями, основанными на открытом исходном коде.

Подсистема WSL (Windows для Linux) позволяет разработчикам запускать среду GNU/Linux с большинством программ командной строки, служебных программ и приложений непосредственно в Windows без каких-либо изменений и необходимости использовать традиционную виртуальную машину или двойную загрузку. Подсистему WSL можно использовать для запуска программ дистрибутива Kali Linux.

Средства сетевого мониторинга Windows

В состав средств сетевого мониторинга Windows входят утилиты, работающие в консольном режиме командной строки. Эти утилиты позволяют проверять доступность удаленных персональных компьютеров (ПК) и диагностировать соединение.

Утилита Arp предназначена для вывода текущих записей в ARP-таблице и определения как IP-адреса, так и аппаратного MAC-адреса.

Утилита Ping предназначена для определения по заданному имени или адресу времени задержки передачи сообщения до указанного ПК. Кроме этого, она позволяет узнать IP-адрес удаленного сервера по его символьному имени. Возможно задание дополнительных параметров: TimeOut – время ожидания ответа на пакет; TTL – время жизни пакета (максимальное число маршрутизаторов, через которые может пройти пакет). Окно утилиты Ping представлено на рис. 2:

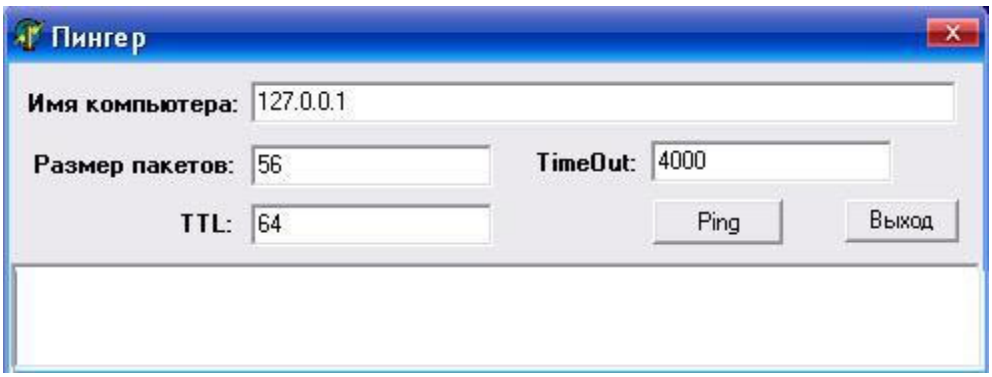

Рис. 2. **Окно утилиты Ping**

Утилита Tracert предназначена для диагностики последовательности межсетевых соединений на пути между двумя ПК.

Утилита PathPing обладает средствами двух упомянутых выше утилит и, кроме того, имеет дополнительные возможности.

Утилита Get IP предназначена для вывода всех установленных IP-адресов для сетевых плат или удаленного доступа для данного ПК. Окна утилит Get IP и Get MAC представлены на рис. 3.

Рис. 3. **Окна утилит Get IP и Get MAC**

Утилита Get MAC для заданного IP-адреса ПК возвращает аппаратный MAC-адрес сетевого устройства ПК, для чего используется протокол NetBIOS.

Утилита WhoIs позволяет получать информацию из огромной базы данных Интернет обо всех доменах всемирной сети. Данные базы расположены на многочисленных узлах сети, например, WWW.NIC.RU, WWW.RIPN.NET, WWW.WHOIS.INTERNIC.NET и т.д. Для доступа к каждой служебной базе используется свой порт. Например, для базы WWW.WHOIS.INTERNIC.NET это порт 43. Утилита имеет поля для ввода адреса базы и номера порта (рис. 4).

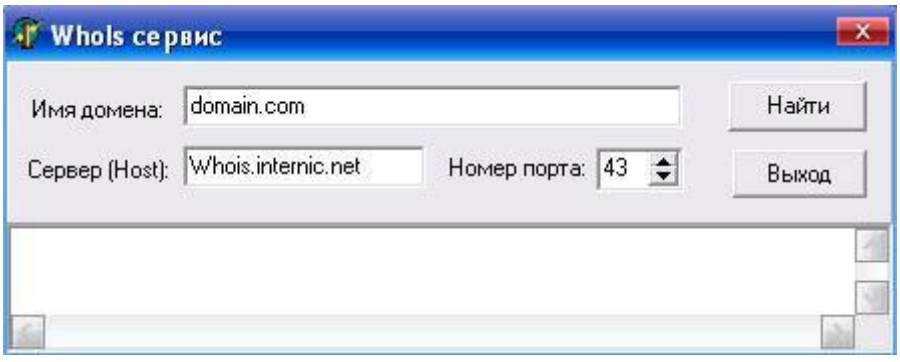

Рис. 4. **Окно утилиты WhoIs**

Утилита Scan Share позволяет производить сканирование сети в поиске доступных (share) ресурсов. В качестве доступных считаются любые ресурсы ПК со свободным доступом из сети (диски, каталоги и принтеры). Сканирование производится для одного IP- адреса.

Утилита Scan Port может сканировать на сервере с заданным IP-адресом по 40 портов сразу (рис. 5). Каждая сетевая программа открывает для себя любой свободный порт.

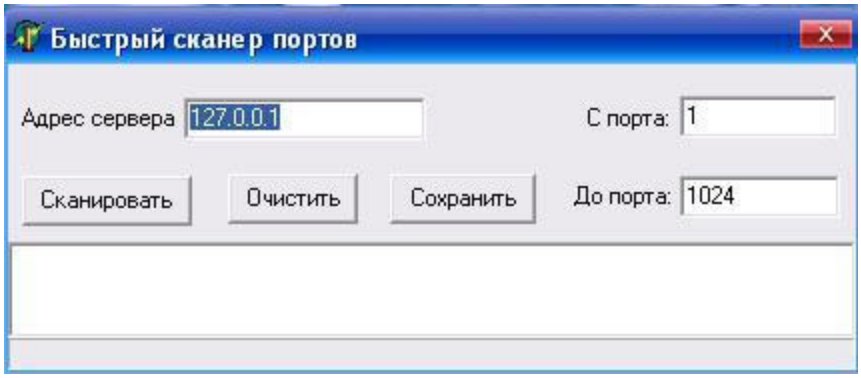

Рис. 5. **Окно утилиты Scan Port**

Если с помощью утилиты Scan Port узнать, какие порты открыты, то можно понять, какие программы запущены на удаленном ПК.

Утилита Net Resource сканирует всю локальную сеть на предмет открытых ресурсов, как это делает сетевое окружение Windows. Можно выбирать различные параметры поиска сетевых ресурсов.

Вывод

Рассмотрены принципы и средства обеспечения безопасности корпоративной сети, а также особенности виртуальных частных сетей, обеспечивающих надежную защиту и защищенную передачу данных.

Рассмотрены системы выявления и предотвращения угроз взлома сети, среди которых основное внимание уделено пакету программ Kali Linux, а также особенности подсистемы Windows для Linux и средства сетевого мониторинга Windows.

Научная новизна исследования, отражающая личный вклад автора, заключается в создании автором компьютерных моделей некоторых утилит мониторинга сети, реализованных в виде программ для ЭВМ с графическим интерфейсом (рис. 2–5).

Список источников

1. Зайцев О.В. Методики обнаружения вредоносного ПО // КомпьютерПресс. 2005. № 6.

2. Зайцев О.В. Шпионские программы как угроза безопасности ПК // КомпьютерПресс. 2008. № 7.

3. Лабинский А.Ю., Ильин А.В. Фракталы и защита информации // Природные и техногенные риски (физико-математические и прикладные аспекты). 2016. № 1. С. 82–86.

4. Лабинский А.Ю. Нейронные сети и защита информации // Проблемы управления рисками в техносфере. 2019. № 1. С. 68–73.

5. Joseph Migga Kizza. Computer Network Security. Springer Science & Business Media, 2005. 535 p.

6. J. Michael Stewart. Network Security, Firewalls and VPNs. Jones & Bartlett Publishers, 2013. 490 p.

7. Sean Convery. Network Security Architectures. Cisco Press, 2004. 739 p.

8. Jie Wang, Zachary A. Kissel. Introduction to Network Security: Theory and Practice. 2015. 440 p.

9. Owen Poole. Network Security. 2007. 224 p.

10. Рафаэль Херцог, Джим О`Горман, Мати Ахарони. Kali Linux от разработчиков. 2018. 320 с.

11. Шива Парасрам, Теди Хериянто, Алекс Замм. Kali Linux. Тестирование на проникновение и безопасность. 2019. 448 с.

References

1. Zajcev O.V. Metodiki obnaruzheniya vredonosnogo PO // Komp'yuterPress. 2005. № 6.

2. Zajcev O.V. Shpionskie programmy kak ugroza bezopasnosti PK // Komp'yuterPress. 2008. № 7.

3. Labinskij A.Yu., Il'in A.V. Fraktaly i zashchita informacii // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty). 2016. № 1. S. 82–86.

4. Labinskij A.Yu. Nejronnye seti i zashchita informacii // Problemy upravleniya riskami v tekhnosfere. 2019. № 1. S. 68–73.

5. Joseph Migga Kizza. Computer Network Security. Springer Science & Business Media, 2005. 535 p.

6. J. Michael Stewart. Network Security, Firewalls and VPNs. Jones & Bartlett Publishers, 2013. 490 p.

7. Sean Convery. Network Security Architectures. Cisco Press, 2004. 739 p.

8. Jie Wang, Zachary A. Kissel. Introduction to Network Security: Theory and Practice. 2015. 440 p.

9. Owen Poole. Network Security. 2007. 224 p.

10. Rafael' Hercog, Dzhim O`Gorman, Mati Aharoni. Kali Linux ot razrabotchikov. 2018. 320 s.

11. Shiva Parasram, Tedi Heriyanto, Aleks Zamm. Kali Linux. Testirovanie na proniknovenie i bezopasnost'. 2019. 448 s.

Информация о статье:
Статья поступила в редакцию: 05.05.2024; одобрена после рецензирования: 25.05.2024;
принята к публикации: 27.05.2024

Information about the article:
The article was submitted to the editorial office: 05.05.2024; approved after review: 25.05.2024;
accepted for publication: 27.05.2024

Информация об авторах:

Лабинский Александр Юрьевич, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат технических наук, доцент, e-mail: labynsciy@yandex.ru, https://orcid.org/0000-0001-2735-4189, SPIN-код: 8338-4230

Information about the authors:

Labinsky Alexander Yu., associate professor of the department of applied mathematics and information technologies of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of technical sciences, associate professor, e-mail: labynsciy@yandex.ru, https://orcid.org/0000-0001-2735-4189, SPIN: 8338-4230