УДК 004.056.53
doi:10.21685/2587-7704-2021-6-1-9

Open Access | RESEARCH ARTICLE

Анализ программных реализаций honeypot-технологий с высоким уровнем взаимодействия

Александр Сергеевич Дёмочкин
Пензенский государственный университет, Россия, г. Пенза, ул. Красная, 40
demochkin2014@gmail.com

Алексей Петрович Иванов
Пензенский государственный университет, Россия, г. Пенза, ул. Красная, 40
ap_ivanov@pnzgu.ru

Аннотация. Проводится обзор существующих программных решений в области высокоинтерактивных honeypot-технологий. Дана краткая характеристика каждого из них. Приведен выбор наиболее эффективной программной реализации honeypot с высоким уровнем взаимодействия.

Ключевые слова: honeypot-технологии, технологии защиты от несанкционируемого доступа, информационная безопасность

Для цитирования: Дёмочкин А. С., Иванов А. П. Анализ программных реализаций honeypot-технологий с высоким уровнем взаимодействия // Инжиниринг и технологии. 2021. Т. 6(1). С. 1–7. doi:10.21685/2587-7704-2021-6-1-9

A survey of software implementation for high-interaction honeypot technologies

Aleksandr S. Demochkin
Penza State University, 40 Krasnaya Street, Penza, Russia
demochkin2014@gmail.com

Aleksey P. Ivanov
Penza State University, 40 Krasnaya Street, Penza, Russia
ap_ivanov@pnzgu.ru

Abstract. A review of the existing software solutions in the field of high-interaction honeypot technologies with a brief description thereof is carried out. The selection of the most efficient high-interaction honeypot software implementation is provided.

Keywords: honeypot technologies, technologies for protection against unauthorized access, information security

For citation: Demochkin A. S., Ivanov A. P. A survey of software implementation for high-interaction honeypot technologies. *Inzhiniring i tekhnologii = Engineering and Technology.* 2021;6(1):1–7. (In Russ.). doi:10.21685/2587-7704-2021-6-1-9

В классификации honeypot-технологий существуют honeypot с низким уровнем взаимодействия (низкоинтерактивные) и с высоким уровнем взаимодействия (высокоинтерактивные) [1].

Honeypot-технологии с высоким уровнем взаимодействия чаще всего представляют собой отдельный хост или устройство, расположенное внутри корпоративной сети, но не участвующее в информационных процессах [1]. Высокоинтерактивные honeypot могут быть представлены как в виде реального хоста, так и виртуального. Такой вид honeypot предназначен не для того, чтобы эмулировать определенные протоколы или службы, а для того, чтобы представлять для злоумышленника видимую систему для атаки.

Такой подход снижает вероятность того, что нарушитель поймет, что действует с нереальной системой, и снизит вероятность компрометации honeypot. Также из honeypot-технологий высокого уровня взаимодействия можно строить целую сеть под названием honeynet. Такая система может со-

© Дёмочкин А. С., Иванов А. П., 2021. Контент доступен по лицензии Creative Commons Attribution 4.0 License / This work is licensed under a Creative Commons Attribution 4.0 License.

ставлять отдельный сегмент в сети организации, которая позволит принять на себя все атаки на корпоративную инфраструктуру, не затронув реальные хосты и не нарушив их работоспособность.

Еще одно преимущество высокоинтерактивных honeypot состоит в том, что они позволяют собирать всю информацию об этапах выполняемых атак, средствах и методах, используемых злоумышленником для несанкционируемого доступа и раскрытия конфиденциальной информации, а также возможных уязвимостях в корпоративной инфраструктуре. Кроме этого, преимуществом honeypot с высоким уровнем взаимодействия является то, что данные средства позволяют сотрудникам отдела безопасности организации быстро реагировать на инциденты безопасности, притом что злоумышленник в это время продолжает производить атаку. Также, в отличие от honeypot с низким уровнем взаимодействия, высокоинтерактивные honeypot могут противостоять атакам «нулевого дня» [2].

Однако honeypot высокого уровня взаимодействия имеют и ряд недостатков. Главный из них заключается в том, что если система в виде honeypot будет скомпрометирована, то она может быть использована как средство для проведения атак «постэксплуатации», т.е. для дальнейшего проникновения в реальную сеть организации, а также закрепления в этой системе. На скомпрометированной honeypot злоумышленник может установить ботнет, что приведет к нарушению безопасности системы. Еще одним недостатком такого вида honeypot является то, что необходимы значительные временные и технические ресурсы для развертывания высокоинтерактивного honeypot, а также хорошая квалификация сотрудников, выполняющих их настройку.

В настоящее время «open-source» проектов в сфере высокоинтерактивных honeypot немного. В рамках данной статьи будут рассмотрены следующие программные решения:

– T-Pot;
– LyreBird;
– DockPot;
– Modern Honey Network (MHN).

Для сравнения указанных выше программных решений был проведен обзор данных высокоинтерактивных honeypot. В статье также рассмотрен разбор установки и настройки каждого ПО для более наглядных результатов сравнительной характеристики, сделаны выводы о возможности компрометации данных honeypot с высоким уровнем взаимодействия.

1. T-Pot – это высокоинтерактивный honeypot, представляющий собой модульную систему из множества docker-контейнеров [3]. Каждый из контейнеров содержит в себе следующие низкоинтерактивные honeypot:

– adbhoney;
– ciscoasa;
– citrixhoneypot;
– dicompot;
– dionaea;
– elasticpot;
– honeypy;
– honeytrap;
– и др.

T-Pot имеет следующие дополнительные инструменты:

– Cockpit – утилита для мониторинга производительности в режиме реального времени и веб-терминала;
– Cyberchef – веб-приложение для шифрования, кодирования, сжатия и анализа данных;
– ELK – инструмент для визуализации в графическом виде данных;
– Elasticsearch – веб-интерфейс для просмотра результатов работы honeypot;
– Fatt – скрипт для извлечения метаданных сети из файлов типа «pcap» и сбора сетевого трафика;
– Spiderfoot – инструмент для автоматизации процесса «OSINT»;
– Suricata – механизм мониторинга сетевой безопасности.

Структура T-Pot представлена на рис. 1.

Установка T-pot может производиться либо с помощью готового ISO-образа, либо в дистрибутиве Debian 10 на основе склонированного git-репозитория. При этом T-pot можно устанавливать как в виде реального хоста, так и в виде виртуальной машины. Единственным условием при установке данного ПО на виртуальную машину является прямое подключение к сети через мост (bridged). Необходимые системные требования для T-pot можно найти в git-репозитории проекта [3]. Вариант установки через готовый ISO-образ не будет рассмотрен в данной статье, важно только уточнить, что

данная установка более проста, нежели с вариантом ручной установки. В любом случае существуют следующие типы установки системы (как при готовом ISO-образе, таки и при ручной установке):

– стандартный – установка всех имеющихся низкоинтерактивных honeypot и инструментов;

– «сенсор» – установка всех низкоинтерактивных honeypot, а также инструментов, кроме ELK;

– промышленный – не подразумевает установку таких honeypot, как dionaea, elasticpot, mailoney;

– «сборщик» – установка только honeypot heralding & honeytrap;

– лечебный – установка программного обеспечения, предназначенного только для защиты от вредоносных программ.

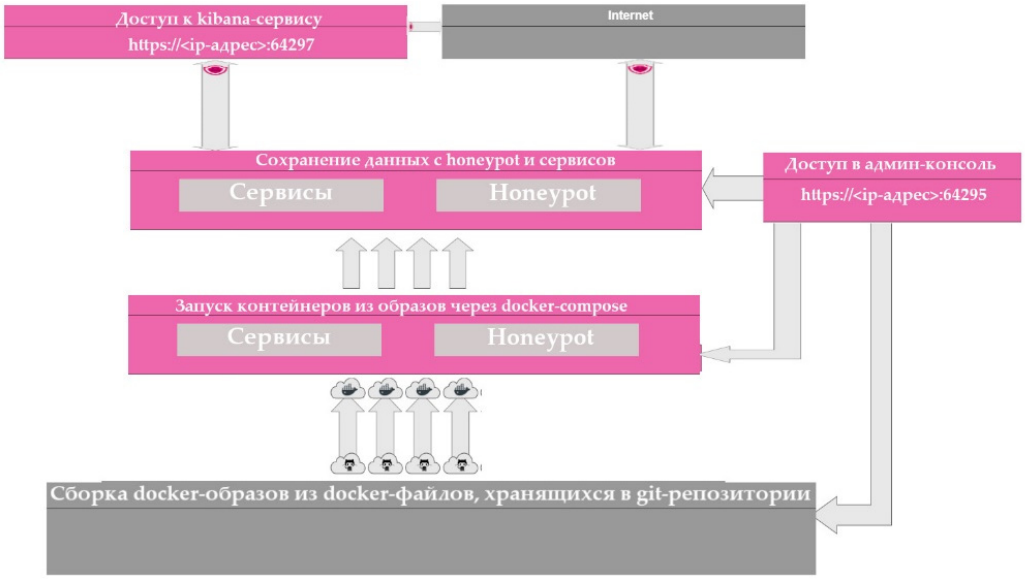

Рис. 1. Архитектура honeypot T-pot

Наиболее подходящий для реального использования является стандартный тип установки. Именно такой и был выбран в рамках проведения исследования T-pot.

Исследования установки и настройки проводились на виртуальной машине, на которой был установлен дистрибутив Linux–Debian 10. В рамках исследования также была сделана попытка установки T-pot на дистрибутив Linux–KaliLinux 20.04, однако при запуске bash-скрипта, отвечающего за установку T-pot, происходит ошибка, которая не дает выполнить установку данного ПО.

Процесс установки системы занял примерно 20–30 мин, при этом процесс первичной настройки системы является достаточно простым. Нужно только создать учетную запись пользователя для дальнейшего входа в веб-интерфейс системы.

После завершения установки T-pot создается два веб-приложения (административная консоль и пользовательская система со всеми инструментами). Доступ к веб-приложениям можно получить через браузер, введя IP-адрес хоста и указав порт, на котором размещена та или иная система.

В результате установки и настройки создается высокоинтерактивный honeypot с открытыми портами в диапазоне от 21 до 65389. В рамках дополнительного конфигурирования некоторые порты можно закрыть. Подробную информацию о нарушителях, проводимых ими атаках можно получить в интерфейсе службы Kibana.

На основе вышеописанной информации можно сделать следующие выводы о данной системе. Достоинством T-pot является его функциональные возможности для развертывания honeypot с высоким уровнем взаимодействия. Данная модульная система имеет множество низкоинтерактивных honeypot, а также дополнительных инструментов для сбора информации о нарушителях и векторах атак. Процесс настройки и установки данной системы не сложен, однако есть недостаток в виде установки либо только из ISO-образа, либо только на дистрибутив Debian 10. На другие дистрибутивы Linux данная система не устанавливается. Кроме этого, в процессе эксплуатации системы было замечено, что некоторые сервисы нестабильно работают, что ухудшает целостность и доступность системы.

Еще одним недостатком является то, что при первоначальной конфигурации системы практически все порты у honeypot с высоким уровнем взаимодействия, созданного при помощи T-pot, будут открыты. Такой вид honeypot в большинстве случаев отпугнет нарушителя, так как в реальности нет таких хостов, где были бы открыты все известные порты.

2. LyreBird – это фреймворк для развертывания honeypot с высоким уровнем взаимодействия [4]. Данное ПО позволяет регистрировать все атаки нарушителей в реальном времени, а также позволяет обнаруживать атаки «человек посередине» из-за специфики своей сборки. Вся информация о векторах атак и злоумышленниках собирается в дамп-файл, а также в html-отчет.

Сама же система представляет собой Docker-контейнер. Пример установки и запуска LyreBird на дистрибутиве KaliLinux 20.04 представлен на рис. 2.

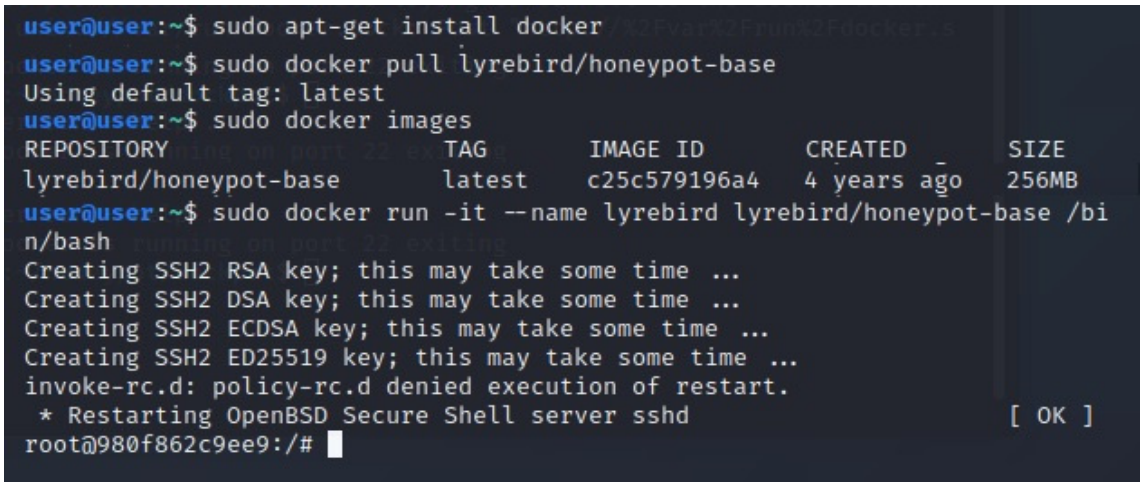

Рис. 2. Процесс развертывания LyreBird

В результате установки LyreBird запускается Docker-контейнер, который представляет из себя высокоинтерактивный honeypot с открытым 22 портом для перехвата атак «человек посередине».

Достоинством данной системы является то, что она собрана в виде docker-образа, который можно развернуть на любом дистрибутиве Linux. Однако документация, приложенная к проекту на ресурсе hub-docker, неактуальна на сегодняшний день. Git-репозиторий проекта LyreBird недоступен, а последнее обновление производилось в 2016 г.

Еще одним плюсом системы является то, что LyreBird – единственный honeypot с высоким уровнем взаимодействия, позволяющий перехватывать атаки типа man-in-the-middle. Скомпрометировать honeypot, созданный с помощью LyreBird, сложно, так как на нем открыт только один 22 порт, отвечающий за ssh-соединение. Все попытки ввести нелегальные данные для авторизации по ssh или провести атаки брутфорса пароля пользователя регистрируются данной системой. Кроме этого, так как LyreBird выполнен в виде docker-образа, то безопасность высокинтерактивного honeypot на его основе также увеличивается. LyreBird во время тестирования стабильно работает, однако при завершении работы с docker-контейнером его необходимо удалить из репозитория запущенных контейнеров и заново собрать.

Недостатком данной системы является сложность ее настройки, так как она уже представлена в готовом docker-контейнере, который сложно пересобрать. Заявленный же в документации к проекту конфигурационный файл docker-compose.yml отсутствует. Кроме этого, при окончании работы LyreBird не создает html-отчет, о котором также говорится в документации.

3. DockPot – это высокоинтерактивный ssh-honeypot, основанный на docker-контейнере. Данное ПО представляет из себя NAT-устройство, которое имеет возможность выступать в качестве ssh-прокси между злоумышленником и honeypot с возможностью регистрации действий злоумышленника [5].

Dockpot основан на honeypot Honssh с некоторыми изменениями для запуска docker-контейнеров при новых соединениях. Кроме этого, Dockpot включает в себя низкоинтерактивные honeypot–Kippo. Процесс установки Dockpot в дистрибутиве KaliLinux 20.04 представлен на рис. 3.

В процессе установки Dockpot необходимо собирать два docker-контейнера, один из которых является ssh-сервером, а другой honeypot Dockpot.

Достоинством Dockpot является то, что он представлен в виде docker-контейнера, что облегчает процесс установки данной системы на любом дистрибутиве Linux. Однако, сравнивая с тем же LyreBird, который также выполнен в виде контейнера, для Dockpot необходимо создать дополнительный docker-контейнер в виде ssh-сервера. Dockpot так же, как и LyreBird, давно не обновлялся, последние изменения проекта на github зафиксированы в 2015 г. Система имеет только открытый 22 порт, со-

брана в виде docker-образа, поэтому скомпрометировать honeypot на его основе будет сложно. Большим недостатком данного решения honeypot с высоким уровнем взаимодействия является то, что данные о злоумышленниках фиксируются только в логах контейнера. Никакого графического представления собранной информации или отчета Dockpot не предусматривает. Также при тестировании Dockpot не всегда стабильно работает, так как docker-контейнер, отвечающий за ssh-сервер, не всегда может установить соединение с docker-контейнером honeypot.

```
user@user:~$ sudo apt-get install docker
user@user:~$ curl -sSL https://get.docker.com/ > installdocker.sh
user@user:~$ sh ./installdocker.sh
user@user:~/honeypot$ git clone https://github.com/aabed/dockpot.git
Клонирование в «dockpot»…
user@user:~/honeypot$ cd dockpot/
user@user:~/honeypot/dockpot$ ./honsshctrl.sh START
```

Рис. 3. Процесс развертывания Dockpot

4. MHN (Modern Honey Network) – это высокоинтерактивный honeypot, представляющий собой централизованный сервер для управления и сбора данных [6]. MHN позволяет быстро развертывать разные сервисы и службы, а также собирать данные, которые можно просматривать с помощью веб-интерфейса. Некоторые сервисы и службы MHN являются honeypot с низким уровнем взаимодействия, такие как Snort, Cowrie, Dionaea, glastopf и др.

Для удобства использования Modern Honey Network собран в виде веб-приложения, написанного на фреймворке Flask [6]. Веб-интерфейс позволяет собирать и разворачивать низкоинтерактивные honeypot, регистрировать и просматривать списки атак, формировать и сохранять отчеты о вторжениях, а также о злоумышленниках. В соответствии с документацией на данное ПО сервер MHN поддерживает работу на дистрибутивах Linux: Ubuntu 18.04, Ubuntu 16.04 и Centos 6.9. Процесс установки, настройки и запуска данной системы представлен на рис. 4.

```
user@ubuntu:~$ sudo apt install git -y
user@ubuntu:/opt$ sudo git clone https://github.com/pwnlandia/mhn.git
Cloning into 'mhn'...
user@ubuntu:/opt$ cd mhn/
user@ubuntu:/opt/mhn$ sudo ./install.sh
Do you wish to run in Debug mode?: y/n n
Superuser email: demochkin2014@gmail.com
Superuser password:
Superuser password: (again):
Server base url ["http://85.234.37.158"]: http://127.0.0.1
Honeymap url ["http://127.0.0.1:3000"]:
Mail server address ["localhost"]:
Mail server port [25]:
Use TLS for email?: y/n n
Use SSL for email?: y/n n
Mail server username [""]:
Mail server password [""]:
Mail default sender [""]:
Path for log file ["/var/log/mhn/mhn.log"]:
+ echo -e '\nInitializing database, please be patient. This can take several minutes'
```

Рис. 4. Процесс развертывания Modern Honey Network

Как показало тестированние данного ПО, время на установку и первоначальную конфигурацию занимает примерно 20–30 мин.

Достоинством MHN является его стабильная работа. Он позволяет в разном виде собирать всю информацию о проводимых атаках на honeypot и выводить пользователю в удобном для него виде в веб-интерфейсе. Еще одним плюсом данного решения honeypot с высоким уровнем взаимодействия является то, что установка и настройка не предполагают больших временных и технических затрат. Также имеется система авторизации пользователя при входе в веб-интерфейс honeypot. Еще одним плюсом данной системы является то, что набор программных компонентов в составе высокоинтерактивного honeypot для сбора информации об атаках и злоумышленниках довольно обширный.

Кроме этого, есть возможность установки Modern Honey Network в виде docker-контейнера. Однако процесс стабильного развертывания MHN возможен только на некоторых дистрибутивах

Linux. Например, на дистрибутиве Kali Linux 20.04 не получится развернуть данный honeypot, так как MHN работает с системой управления пакетами python-pip, а в Kali Linux 20.04 возможна работа только с версией python-pip3.

Общая сравнительная характеристика реализаций honeypot-технологий с высоким уровнем взаимодействия представлена в табл. 1.

Таблица 1

Сравнение программных решений высокоинтерактивных honeypot

Программная реализация	Характеристика			
	Функциональные возможности	Простота настройки и установки	Удобство использования	Уровень возможной компрометации
T-Pot	Высокие. Имеет большое количество низкоинтерактивных honeypot и инструментов для сбора информации об атаках и злоумышленниках	Высокая. Имеет готовый iso-образ для развертывания, а также есть возможность установки на готовый дистрибутив Linux	Высокая степень. Существует веб-приложение с разными инструментами, которые позволяют отслеживать всю информацию об злоумышленниках и проводимых ими атаках в разном представлении (таблицы, графики и т.д.)	Высокий. При первоначальной конфигурации honeypot имеет более 6000 открытых портов. Не используется технология контейнеризации
Lyrebird	Средние. Достоинством данной реализации является то, что данная реализация может перехватывать атаки «человек посередине»	Средняя. Установка данной системы происходит через docker-контейнер. Однако существует сложность при изменении конфигурационного файла honeypot в связи со спецификой docker-образа	Низкая. Информация с honeypot собирается только в дамп-файл. Заявленный в документации на проект процесс создания html-отчета не работает	Низкий в силу использования технологии контейнеризации, а также использование только ssh-порта для отслеживания проводимых на систему атак
Dockpot	Низкие. Есть только возможности по прослушиванию ssh-сессий	Низкая. Необходимо развернуть два docker-контейнера, при этом не каждый docker-образ ssh-сервера подойдет для контейнера системы Dockpot	Низкая. Информация о проводимых атаках и злоумышленниках можно наблюдать только в лог-файлах	Низкий в связи с использованием технологии контейнеризации
MHN	Высокие. Имеет достаточное количество низкоинтерактивных honeypot и инструментов для фиксации проводимых на систему атак (более 15 разновидностей)	Высокая. Установка происходит с помощью bash-скрипта, при запуске которого можно указать все необходимые конфигурационные данные для развертывания системы	Высокая. Используется веб-приложение для подробного анализа собранной информации с honeypot	Средний. Первоначально система устанавливается на реальную систему с веб-приложением, которое можно скомпрометировать. Однако существует возможность запуска и установки MHN в виде docker-контейнера

На основе описания каждой программной реализации, а также сравнительной характеристики можно сделать вывод, что наиболее эффективным honeypot с высоким уровнем взаимодействия для применения в условиях реальной системы будет высокоинтерактивный honeypot-система Modern Honey Network. Процесс ее установки и настройки довольно прост. Система может устанавливать как на готовую систему под управлением ОС Ubuntu Linux или Centos, так и в виде docker-контейнера. Также плюсом данной системы является то, что на сегодняшний день она поддерживается разработ-

чиками, выходят новые версии (в отличие от Dockpot и Lyrebird). Кроме этого, как показал опыт, MHN работает более стабильно, чем программная реализация высокинтерактивного honeypot / T-pot. По функциональным возможностям данные системы примерно одинаковы, однако MHN в первоначальной конфигурации имеет меньший уровень возможной компрометации.

Список литературы

1. Intrusion Detection FAQ: What is a Honeypot? URL: https://www.sans.org/security-resources/idfaq/honeypot3.php (дата обращения: 05.02.2021).
2. Compte Rendude Projet Étudedes Honeypots. URL: https://arthurbachelet.me/assets/Project/Files/Honeypots.pdf (дата обращения: 05.02.2021).
3. T-Pot 20.06. URL: https://github.com/telekom-security/tpotce (дата обращения: 05.02.2021).
4. Lyrebirdis: A high-interaction honeypot framework. URL: https://hub.docker.com/r/lyrebird/honeypot-base/ (дата обращения: 05.02.2021).
5. Dockpot - high interaction SSH honeypot. URL: https://www.honeynet.org/projects/active/dockpot/ (дата обращения: 05.02.2021).
6. Modern Honey Network. URL: https://github.com/pwnlandia/mhn (дата обращения: 05.02.2021).

References

1. *Intrusion Detection FAQ: What is a Honeypot?* Available at: https://www.sans.org/security-resources/idfaq/honeypot3.php (accessed 05.02.2021).
2. *Compte Rendude Projet Étudedes Honeypots*. Available at: https://arthurbachelet.me/assets/Project/Files/Honeypots.pdf (accessed 05.02.2021).
3. *T-Pot 20.06*. Available at: https://github.com/telekom-security/tpotce (accessed 05.02.2021).
4. *Lyrebirdis: A high-interaction honeypot framework*. Available at: https://hub.docker.com/r/lyrebird/honeypot-base/ (accessed 05.02.2021).
5. *Dockpot - high interaction SSH honeypot*. Available at: https://www.honeynet.org/projects/active/dockpot/ (accessed 05.02.2021).
6. *Modern Honey Network*. Available at: https://github.com/pwnlandia/mhn (accessed 05.02.2021).

Поступила в редакцию / Received 28.01.2021

Поступила после рецензирования и доработки / Revised 04.03.2021

Принята к публикации / Accepted 15.03.2021