

Лабораторная работа № 2

Проведение фишинговой атаки

Выполнили: Завьялова В.В, Ким С.Е, Казачкова О.В.

Группа: Б9118-09.03.04прогин(2).

Цель работы: проведение фишинговых атак на почты gmail.com, mail.ru, students.dvfu.ru со следующими критериями:

1. Первое письмо должно содержать документ со скриптом, отсылающий на сервер информацию о запущенной системе (canarytoken). Тема атаки – атака на отдел кадров ДВФУ.
2. Второе письмо должно содержать ссылку, при переходе по которой пользователь попадает на фишинговый сайт, содержащий копию формы авторизации сайта Steam.
3. Промежуток между отправкой писем должен составлять 24 часа и каждое письмо отсылается в 21:00 по UTC.
4. Содержимое письма, заголовок и подпись должны максимально соответствовать выбранной тематики письма.

Работа проводила в три дня, в каждый из которых рассыпались письма различной тематики.

Был создан сервер на www.digitalocean.com для работы с Gophish.



ubuntu-s-1vcpu-1gb-sgp1-01

in  veronicazzzz / 1 GB Memory / 25 GB Disk / SGP1 - Ubuntu 20.04 (LTS) x64

ipv4: 159.223.94.46

ipv6: [Enable now](#) Private IP: 10.104.0.3

Floating IP: [Enable now](#)

Также было зарегистрировано бесплатное доменное имя на www.noip.com

| Hostname ▲ | Last Update | IP / Target |
|--|-----------------------------|---------------|
|  steamservice.sytes.net Active | Dec 16, 2021 03:28 PST ⓘ | 159.223.94.46 |

В качестве отправителя использовалась почта yandex.ru, как наиболее простая в процессе настройки параметров безопасности.

День первый

Организация фишинговой рассылки от лица поддержки Steam.

Name:

SteamServer

Interface Type:

SMTP

From:

Поддержка Steam<securityelena@yandex.ru>

Host:

smtp.yandex.com:465

Username:

securityelena@yandex.ru

Password:

Создание SMTP сервера для рассылки от Steam

Письмо, отправленное пользователям, имеет следующий вид:



Здравствуйте,

**Ваш аккаунт Steam был заморожен из-за
подозрительной попытки входа.**

ВОССТАНОВИТЬ ДОСТУП

Вы получили это письмо из-за попытки входа с компьютера по адресу 23.106.56.14 (UK). При входе были введены верные логин и пароль.

Если вы не пытались войти в свой аккаунт, измените пароль аккаунта Steam. Также стоит сменить пароль эл. почты, чтобы обеспечить защиту своего аккаунта.

С уважением,
команда Steam

Это уведомление отправлено на адрес эл. почты, связанный с вашим аккаунтом Steam.

Это письмо сгенерировано автоматически. Пожалуйста, не отвечайте на него. Если вам понадобится помочь, обратитесь в службу поддержки Steam.

<https://help.steampowered.com>



Чтобы установить настольный клиент Steam и узнать больше, перейдите на вкладку «О Steam».

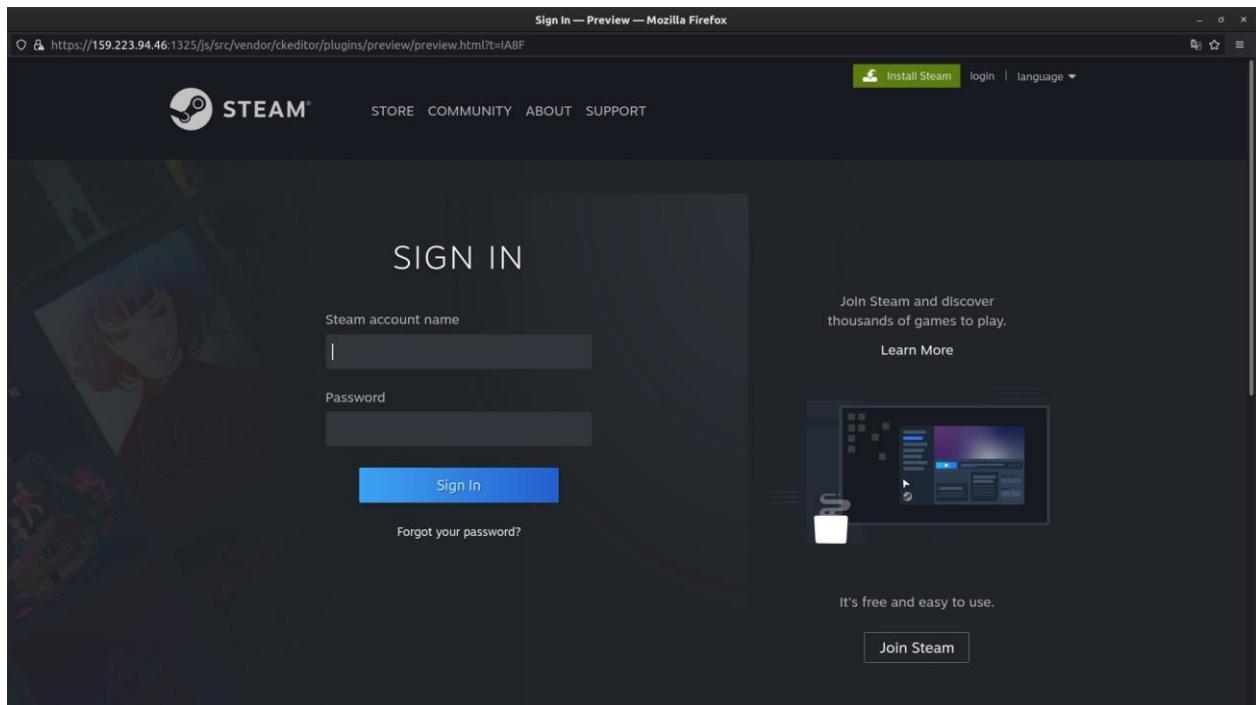
[О Steam](#)



© Valve Corporation
PO Box 1688 Bellevue, WA 98009

Все права защищены. Все торговые марки являются собственностью соответствующих владельцев в США и других странах.

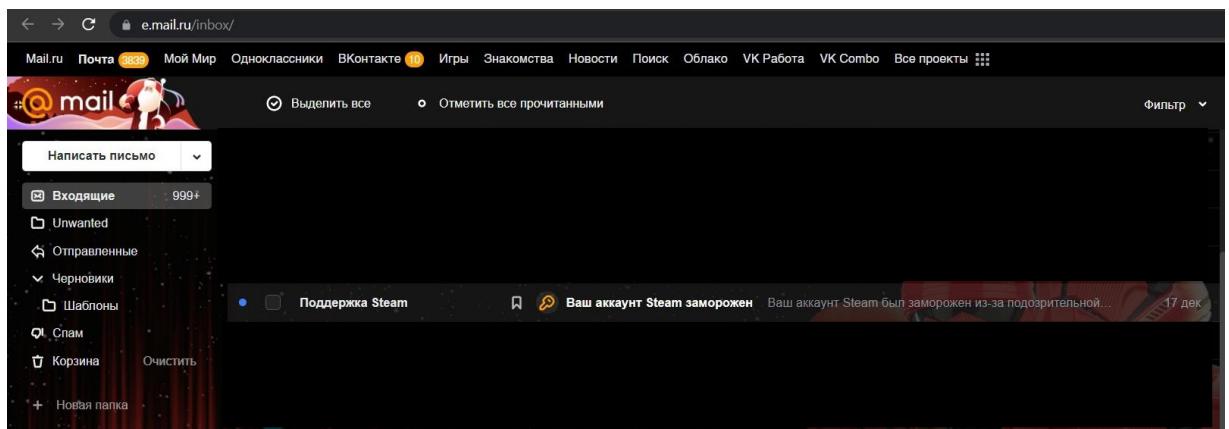
Кнопка «Восстановить доступ» содержит ссылку, ведущую на landing page, с переадресацией на главную страницу Steam.



Данная рассылка проводилась на почты gmail.com и mail.ru

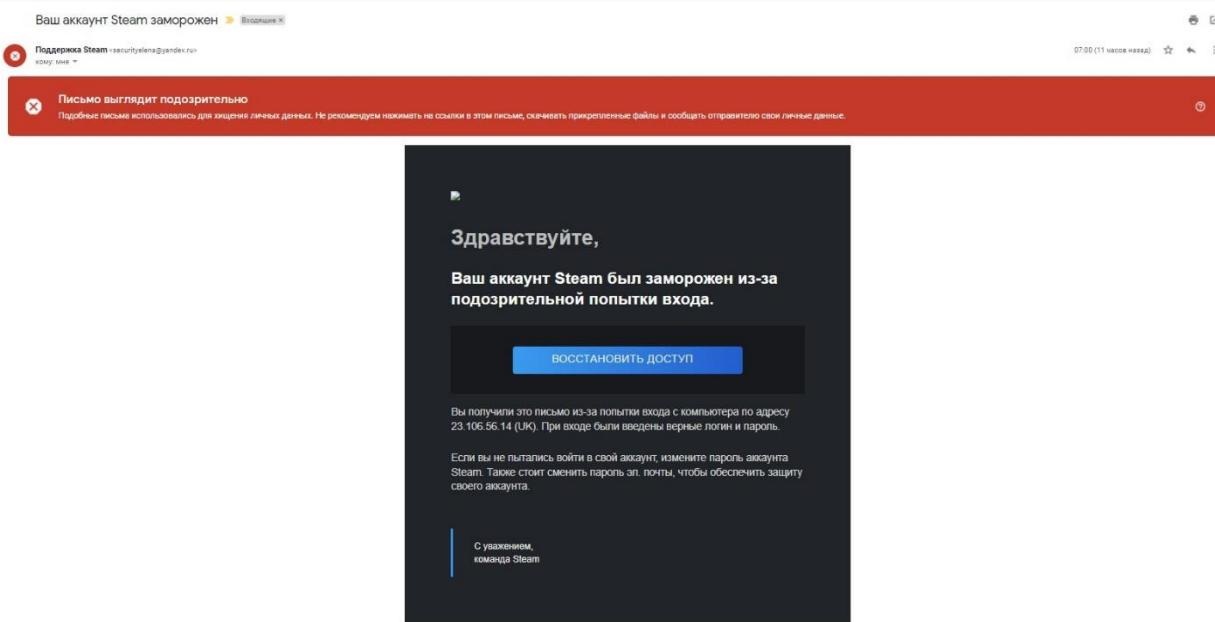
mail.ru

Письмо не попало в спам, и осталось в основной папке Входящие:

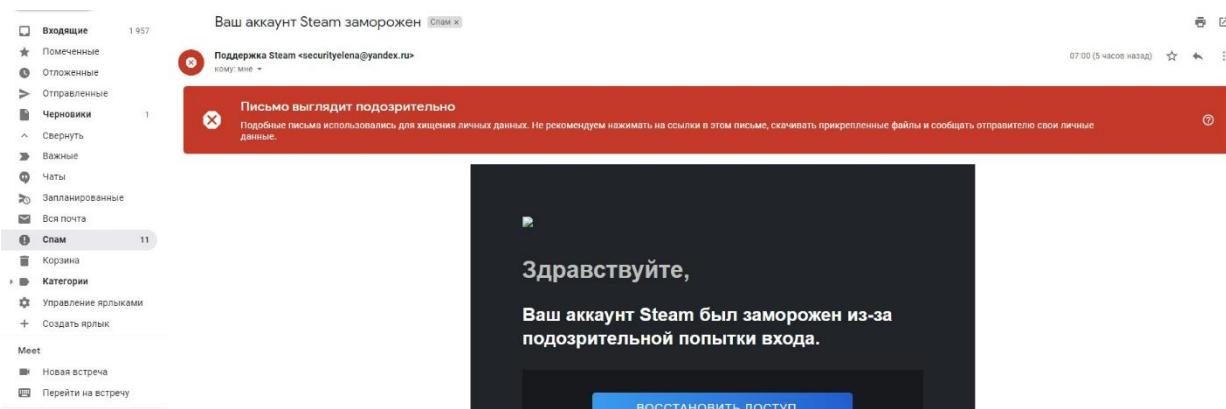


gmail.com

В 4 из 5 случаев письмо осталось в папке Входящие, однако, в некоторых случаях к письму была прикреплена пометка о его подозрительности.



В 1 случае из 5 письмо попало в спам.



Такое поведение, скорее всего, обусловлено разницей в настройках безопасности каждого отдельного аккаунта.

День второй

Рассылка письма, содержащего документ со скриптом.

Name:
FefuServer

Interface Type:
SMTP

From:
Поддержка ДВФУ<securityelena@yandex.ru>

Host:
smtp.yandex.com:465

Username:
securityelena@yandex.ru

Password:
.....

Создание SMTP сервера для рассылки от ДВФУ

Отправленное пользователям письмо имеет следующий вид:



Также к письму прилагался документ .xlsx со скриптом, созданный с помощью canarytokens.org/generate

Данная рассылка осуществлялась исключительно на корпоративные почты outlook.

Все отправленные письма попали в спам, однако, в 75% случаев файл удалось скачать и запустить без отключения антивируса. Вследствие чего были получены уведомления следующего вида:

Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 82.162.1.104.

Basic Details:

| | |
|----------------|---|
| Channel | HTTP |
| Time | 2021-12-18 13:19:24 (UTC) |
| Canarytoken | 4g9e20mf973nlo7voltncckl |
| Token Reminder | птичка в клетке |
| Token Type | ms_excel |
| Source IP | 82.162.1.104 |
| User Agent | Mozilla/4.0 (compatible; ms-office; MSOffice rmj) |

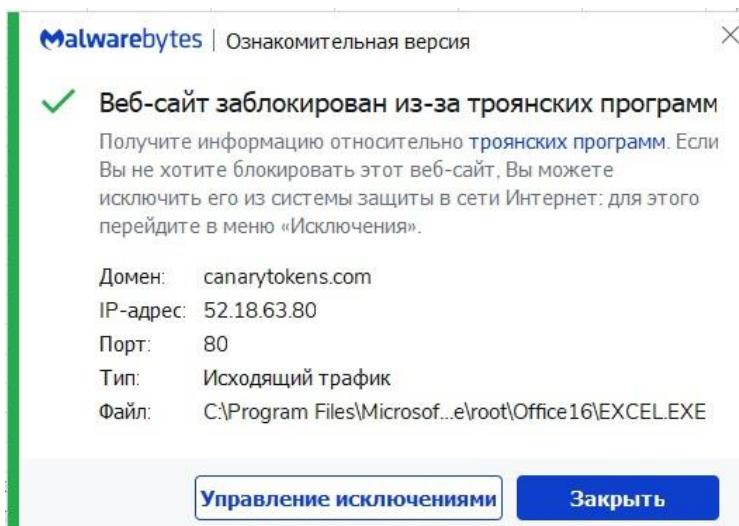
Canarytoken Management Details:

[Manage this Canarytoken here](#)

[More info on this token here](#)

Powered by: [Thinkst Canary](#)

Однако, в одном случае скачать и открыть файл не удалось:

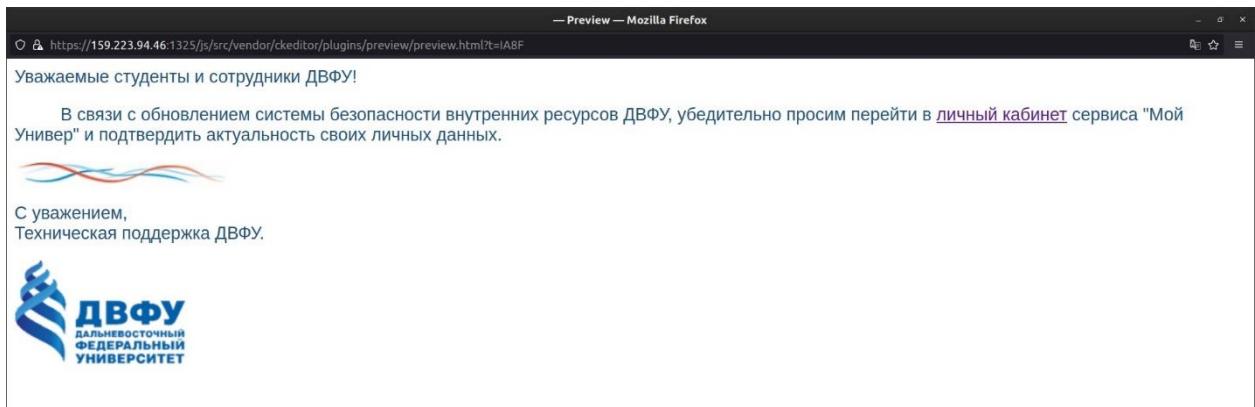


День третий

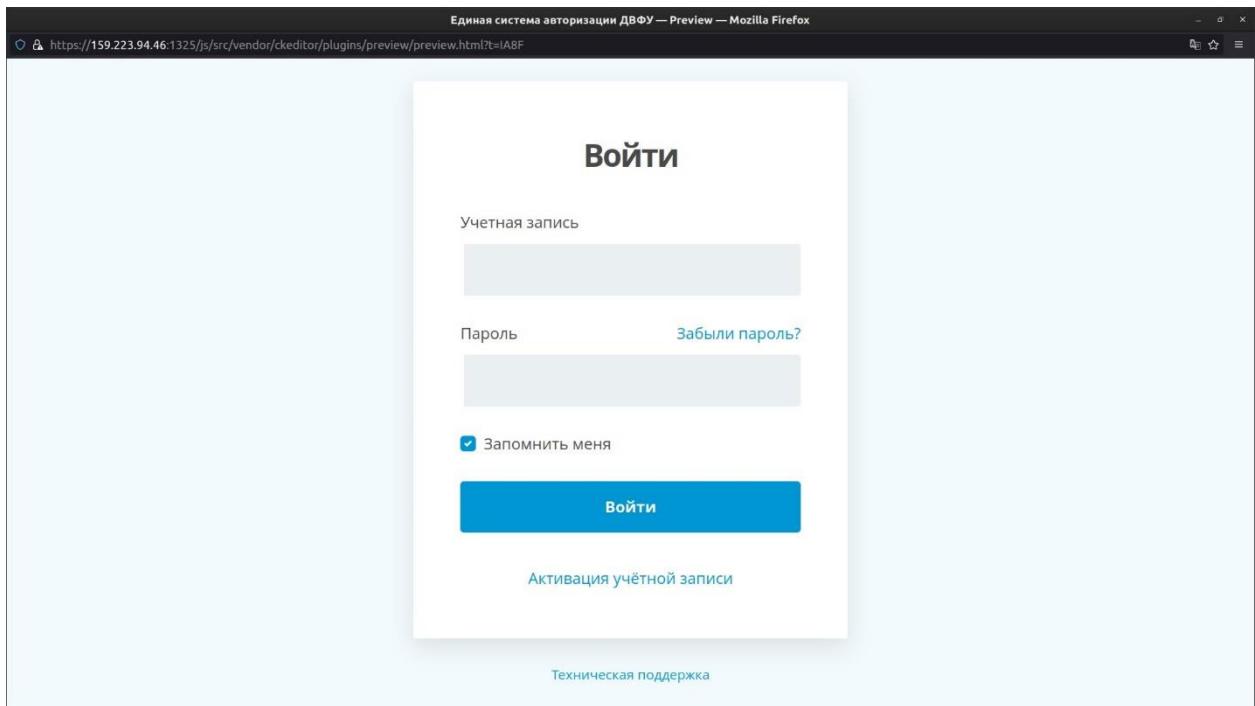
Была проведена еще одна фишинговая рассылка от лица ДВФУ, однако, на этот раз нацеленная не на сотрудников, а на студентов.

Использовался тот же SMTP сервер, что и для предыдущей рассылки от ДВФУ.

Письмо, отправленное пользователям, имеет вид:



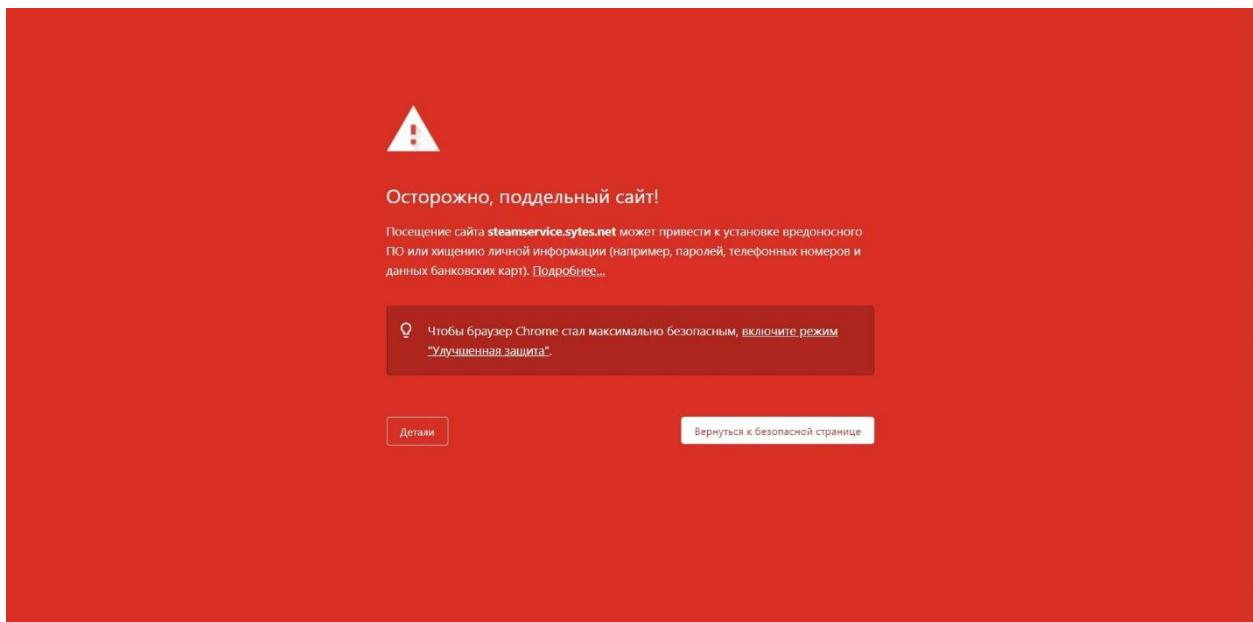
Ссылка из письма ведет на landing page (+ переадресация на сайт ДВФУ):



Данная рассылка осуществлялась как на почты outlook, так и на gmail.com

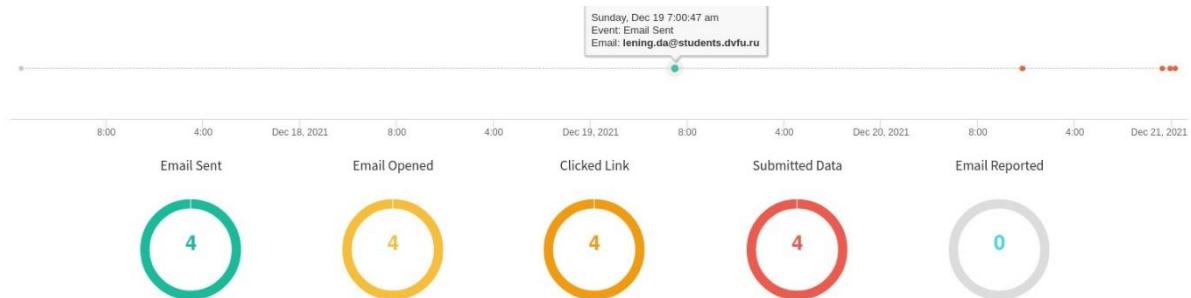
Всего было отправлено 4 письма. 3 из 4 попали в спам (gmail.com в т. ч.), 1 – в общую папку.

Поскольку все пользователя использовали браузер Chrome, при переходе по ссылке возникало уведомление:



Однако, при проверке этой рассылки в Mozilla, никакого предупреждения не возникало.

В ходе данной фишинговой рассылки удалось собрать введенные пользователями данные (Steam, к сожалению, этого сделать не позволил).



Details

| Details | | | | | |
|------------|--|-----------|----------------------------|----------|-----------------------------|
| First Name | | Last Name | Email | Position | Status |
| ▶ | | | lening.da@students.dvfu.ru | CEO | Submitted Data |
| ▶ | | | pravoi.is@students.dvfu.ru | CEO | Submitted Data |
| ▶ | | | sakhakaktus@gmail.com | CEO | Submitted Data |
| ▶ | | | kim.sue@students.dvfu.ru | CEO | Submitted Data |

```
9
10 <a href="https://idm.dvfu.ru/menu/view"></a>, "password": ["polzut"], "rememberMe": ["1"], "rid": ["u8pqXio"], "username": ["glazza"]}, "browser": {"address": "82.162.0.174", "user-agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 YaBrowser/21.12.2.134 Yowser/2.5 Safari/537.36"}, "date": "2021-12-19T07:00:47.000Z", "event": "Email Sent", "email": "lening.da@students.dvfu.ru", "eventTime": "2021-12-19T07:00:47.000Z", "id": 1, "ip": "82.162.0.174", "isMobile": false, "language": "ru_RU", "os": "Windows", "platform": "Windows", "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 YaBrowser/21.12.2.134 Yowser/2.5 Safari/537.36"}, "11
12
13
14
15
16
17
18
19
```