



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение  
высшего образования**

**«Дальневосточный федеральный университет»**

**ИМКТ**

**Департамент информационной безопасности**

**Тананов Алексей Александрович  
Жуков Владимир Владимирович**

**М9120-09.04.02ибкфс**

**ЛР № 2**

**«Проведение фишинговой атаки»**

**г. Владивосток**

**2022**

### **Постановка задачи:**

Провести 2 фишинговые атаки на почты gmail.com, mail.ru, dvfu.ru, protonmail.com со следующими критериями:

1. Первое письмо должно содержать документ с скриптом, отсылающий на сервер информацию о запущенной системе (canarytoken)
2. Второе письмо должно содержать ссылку, при переходе по которой пользователь попадает на фишинговый сайт, содержащий копию формы авторизации. Форма авторизации берется на ваш выбор: двфу outlook, почтовый сервис mail, steam, Instagram, twitter.
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 тематике письма

Почты, используемые в лабораторной работе:

laoratornaadv1@protonmail.com: <pass>

laoratornaadv2@protonmail.com: <pass>

laoratornaadv3@protonmail.com: <pass>

laoratornaadv4@protonmail.com: <pass>

laoratornaadv5@protonmail.com: <pass>

laoratornaadv6@protonmail.com: <pass>

laoratornaadv1@gmail.com: <pass>

laoratornaadv2@gmail.com: <pass>

laoratornaadv3@gmail.com: <pass>

laoratornaadv4@gmail.com: <pass>

laoratornaadv5@gmail.com: <pass>

laoratornaadv1@mail.ru: <pass>

laoratornaadv2@mail.ru: <pass>

laoratornaadv3@mail.ru: <pass>

laoratornaadv4@mail.ru: <pass>

laoratornaadv5@mail.ru: <pass>

tananov.aa@dvfu.ru

zhukov.vvl@dvfu.ru

shapovalova.aal@students.dvfu.ru

gorbonos.nv@students.dvfu.ru

irgit.aa@students.dvfu.ru

## Тематика писем:

Атака на отдел кадров. Письмо содержит информацию о изменении телефонов подразделений ДВФУ. Отсылается от имени одного из менеджеров ДВФУ.

## Письмо 1:

Добрый день!

В связи со вступившими в силу изменениями внутренних номеров телефонов подразделений ШЭМ прошу ознакомиться с прикрепленным документом и принять сведения к работе.

С уважением,  
Холодкова Наталья Васильевна

Главный менеджер  
Административный отдел  
Школа экономики и менеджмента

## Вложенный документ:



Утверждено приказом

от 10.01.2022 №12-34-5678

## Уважаемые коллеги!

С 10.01.2022 вступили в силу изменения следующих вн. номеров:

- Департамент экономических наук: вн.: 2929
- Отдел реализации общественного питания: вн.: 2828
- Лабораторный комплекс ветеринарно-санитарной экспертизы: вн.: 2725
- Департамент менеджмента и предпринимательства: вн.: 2626
- Департамент туризма и гостеприимства: вн.: 2525
- Департамент финансов: вн.: 2424
- Административный отдел: вн.: 2323
- Дирекция: вн.: 2121

## Письмо 2:

Добрый день!

Подтвердите пожалуйста, что ознакомились с предыдущим письмом и приняли в работу данные о изменении вн. номеров телефонов подразделений ШЭМ ДВФУ ответным письмом по следующей ссылке:  
<http://dvfu.sytes.net?rid=6kzeFos>

С уважением,  
Холодкова Наталья Васильевна

Главный менеджер  
Административный отдел  
Школа экономики и менеджмента

Был настроен GoPish, в качестве фишинговой страницы выбран outlook:

## New Group



Name:

Emails

[+ Bulk Import Users](#)

[Download CSV Template](#)

First Name

Last Name

Email

Position

[+ Add](#)

Show  entries

Search:

First Name	Last Name	Email	Position	
g	1	laoratornaadva...	1	
g	2	laoratornaadva...	2	
g	3	laoratornaadva...	3	
g	4	laoratornaadva...	4	
g	5	laoratornaadva...	5	
o	1	tananov.aa@dv...	6	
o	2	zhukov.vvl@dvf...	7	
o	3	shapovalova.aal...	8	
o	4	gorbonos.nv@s...	9	
o	5	irgit.aa@studen...	10	

Showing 1 to 10 of 20 entries

Previous

1

2

Next

Close

Save changes

# New Template



Name:

letter\_1

Import Email

Subject:

Изменение данных подразделений ШЭМ ДВФУ

Text

HTML

Добрый день!  
В связи со вступившими в силу изменениями внутренних номеров телефонов подразделений ШЭМ прошу ознакомиться с прикрепленным документом и принять сведения к работе.

С уважением,  
Холодкова Наталья Васильевна

Главный менеджер  
Административный отдел  
Школа экономики и менеджмента

☐ Add Tracking Image

Add Files

Show  entries

Search:

Name



Подразделения ДВФУ (Изменения от 10.01.2022).docx



Showing 1 to 1 of 1 entries

Previous

1

Next

# New Template



Name:

letter\_2

 Import Email

Subject:

Подтверждение вступивших в силу изменений вн. номеров ШЭМ

Text

HTML

Добрый день!

Подтвердите пожалуйста, что ознакомились с предыдущим письмом и приняли в работу данные о изменении вн. номеров телефонов подразделений ШЭМ ДВФУ ответным письмом по следующей ссылке:

{{.URL}}

С уважением,  
Холодкова Наталья Васильевна

Главный менеджер

☐ Add Tracking Image

 Add Files

Show  entries

Search:

Name

No data available in  
table

Showing 0 to 0 of 0 entries

Previous

Next

# New Sending Profile



Name:

Google

Interface Type:

SMTP

From:

it-help@dvfu.sytes.net

Host:

smtp.gmail.com:25

Username:

adm.dvfu2@gmail.com

Password:

.....

☒ Ignore Certificate Errors

Email Headers:

X-Custom-Header

{{.URL}}-gophish

+ Add Custom Header

Show

10

entries

Search:

Header	Value
No data available in table	

Showing 0 to 0 of 0 entries

Previous

Next

Send Test Email



# New Landing Page



Name:

login dvfu

Import Site

HTML

```
<!DOCTYPE html><html lang="ru-RU"><head>
  <base href="https://fs.dvfu.ru/adfs/ls/?client-request-id=c116635e-b67e-7603-6a85-22e91399f3aa&username=&wa=wsignin1.0&wrealm=urn%3afederation%3aMicrosoftOnline&wctx=estsredirect%3d2%26estsrequest%3drQIIAY2ROWzTUACG_eLUTQKIiEtsVBUTyM17TuxXR2IIuXCT5m4OSxA1PupcfiG-og5sIBZQVzowMEZMDAhVDDA2U-ZOjIUJwcJIIhY2-IZf__p__x0aRVDiNvwDx66ThbgOWEVbt7-YXgmFHyk3Pj95T7uDp9tfr776OT8Gm6qrO5GpMwe3DNueWI1o1Dj2iJBhhOh6X9EiCh1HideNfgBgCcA5AH" />
</head>
```

☒ Capture Submitted Data

☒ Capture Passwords

**Warning:** Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to:

<https://outlook.office.com/mail/>

Cancel

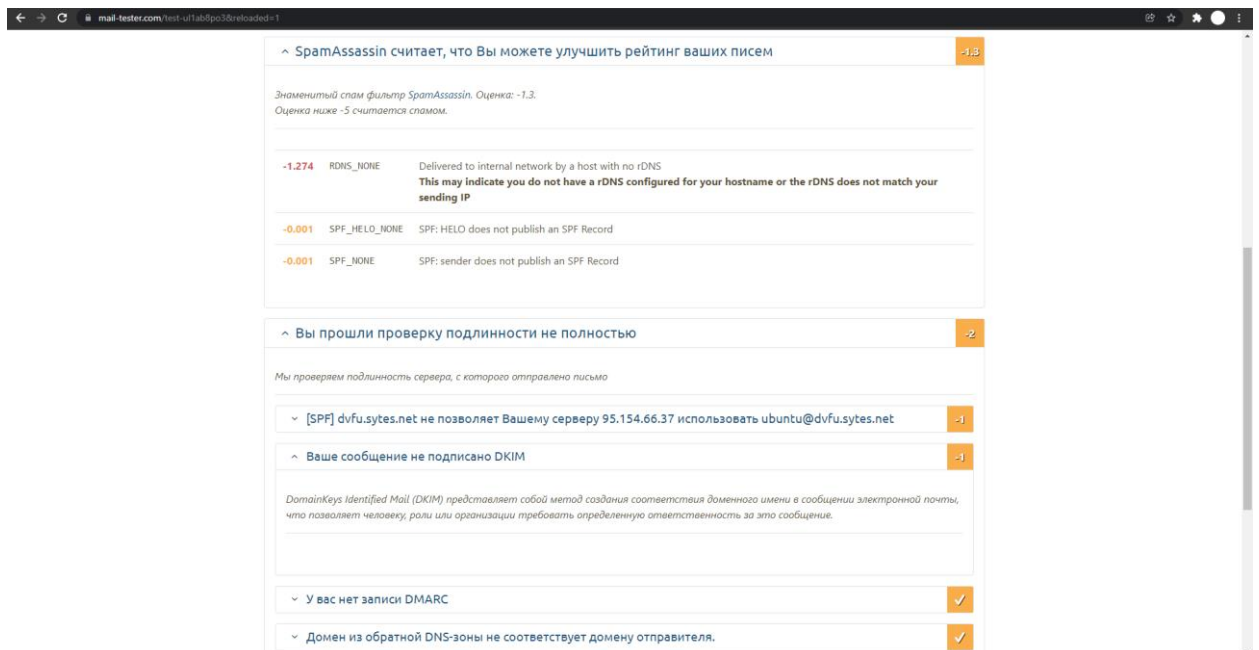
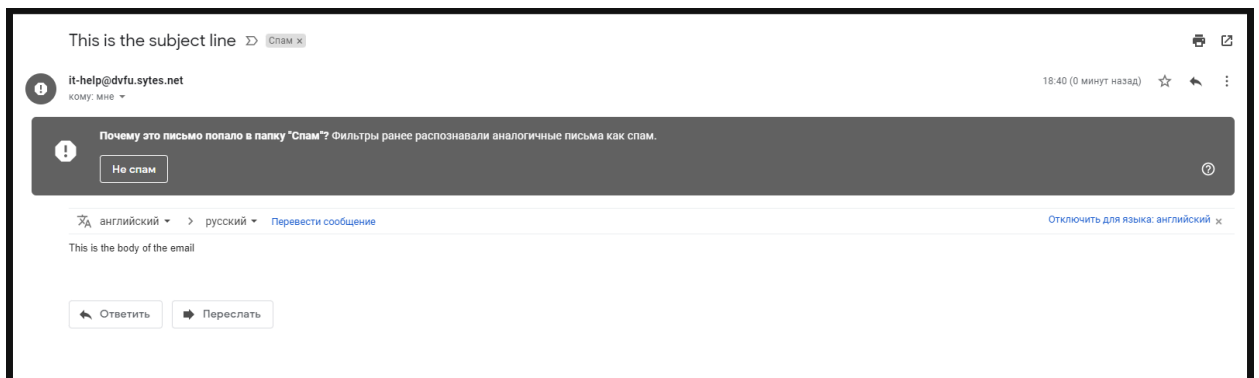
Save Page

Был настроен SMTP сервер и зарегистрировано бесплатное доменное имя, однако письма, рассылаемые с бесплатного доменного имени, попадали в спам.

```
ubuntu@dvmfu: ~
ubuntu@dvmfu:~$ sudo systemctl restart postfix
ubuntu@dvmfu:~$ sudo systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
   Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor prese
   Active: active (exited) since Mon 2022-01-17 08:38:18 UTC; 5s ago
   Process: 35124 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 35124 (code=exited, status=0/SUCCESS)

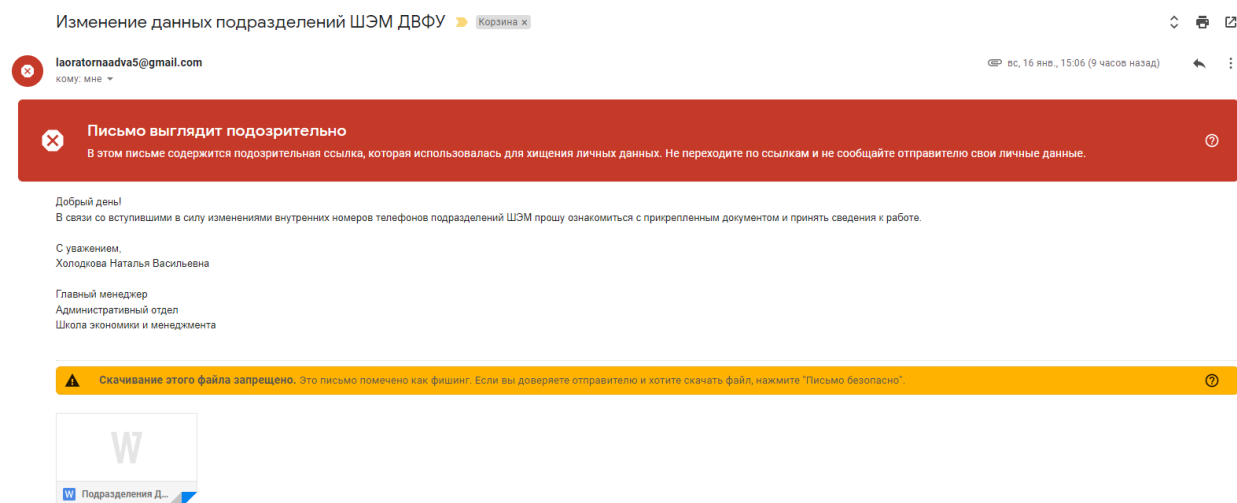
Jan 17 08:38:18 dvmfu.sytes.net systemd[1]: Starting Postfix Mail Transport Agen
Jan 17 08:38:18 dvmfu.sytes.net systemd[1]: Finished Postfix Mail Transport Agen
...skipping...

ubuntu@dvmfu:~$ su it-help
Password:
$ echo "This is the body of the email" | mail -s "This is the subject line" zhuk
ov.vvl@dvmfu.ru
$ echo "This is the body of the email" | mail -s "This is the subject line" ktsv
nn@gmail.com
you have mail
$
```

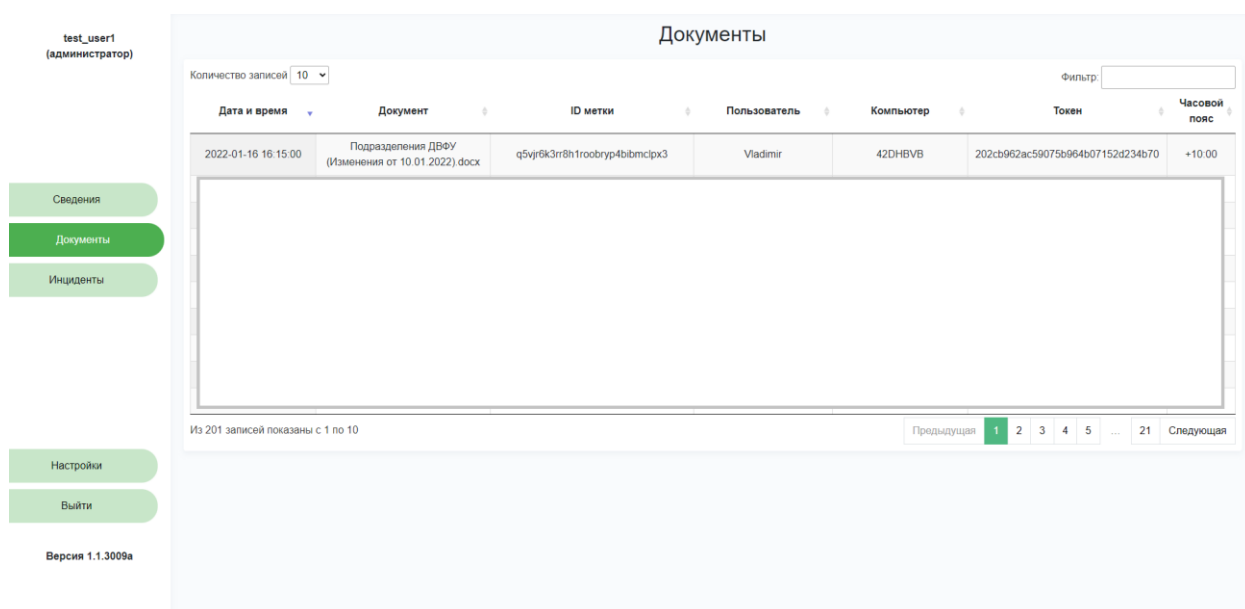


Поэтому основная рассылка осуществлялась с gmail.

При использовании canarytoken gmail выдавал предупреждение об опасности:



Поэтому мы использовали другой проект (в котором принимали участие как разработчики) для получения данных при открытии документа:



В итоге были получены письма (в спам не попали):

Outlook interface showing an email thread. The selected email is titled "Изменение данных подразделений ШЭМ ДВФУ" and is from adm.dvfu2@gmail.com, dated 19.01.2022, 7:01. The email content includes a greeting, a reference to a previous email, and a request to review a document regarding internal telephone department numbers. The sender is identified as Наталья Васильевна, Head Manager of the Administrative Department of the School of Economics and Management.

Outlook interface showing the previous email in the thread, titled "Подтверждение вступивших в силу изменений вн. номеров ШЭМ". It is also from adm.dvfu2@gmail.com, dated 19.01.2022, 7:00. The content includes a greeting, a reference to a previous email, and a request to confirm the implementation of changes to internal telephone department numbers. A link is provided for more information.

Isolated view of the email "Изменение данных подразделений ШЭМ ДВФУ" from adm.dvfu2@gmail.com. The email content is identical to the one shown in the Outlook interface, including the greeting, reference to a previous email, and the request to review a document regarding internal telephone department numbers. The sender is identified as Наталья Васильевна, Head Manager of the Administrative Department of the School of Economics and Management.

## Подтверждение вступивших в силу изменений вн. номеров ШЭМ



adm.dvfu2@gmail.com

20.01.2022, Чт, 7:00

Кому: Тананов Алексей Александрович

Добрый день!

Подтвердите пожалуйста, что ознакомились с предыдущим письмом и приняли в работу данные о изменении вн. номеров телефонов подразделений ШЭМ ДВФУ ответным письмом по следующей ссылке:  
<http://dvfu.sytes.net?rid=6kzeFos>

С уважением,

Холодкова Наталья Васильевна

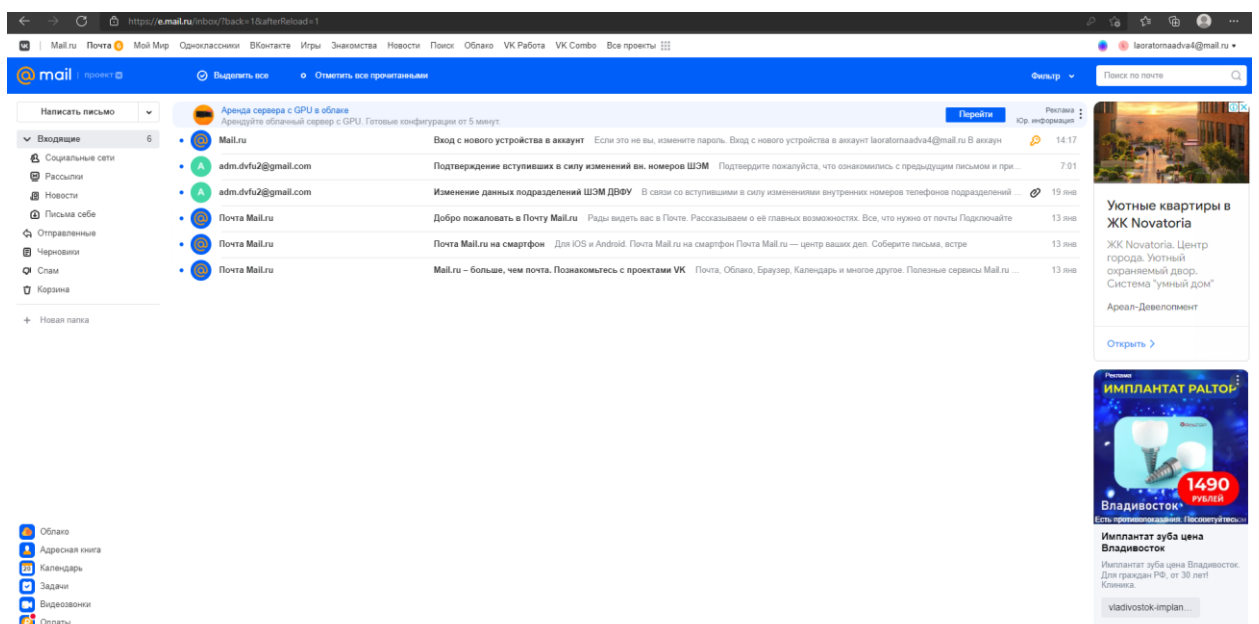
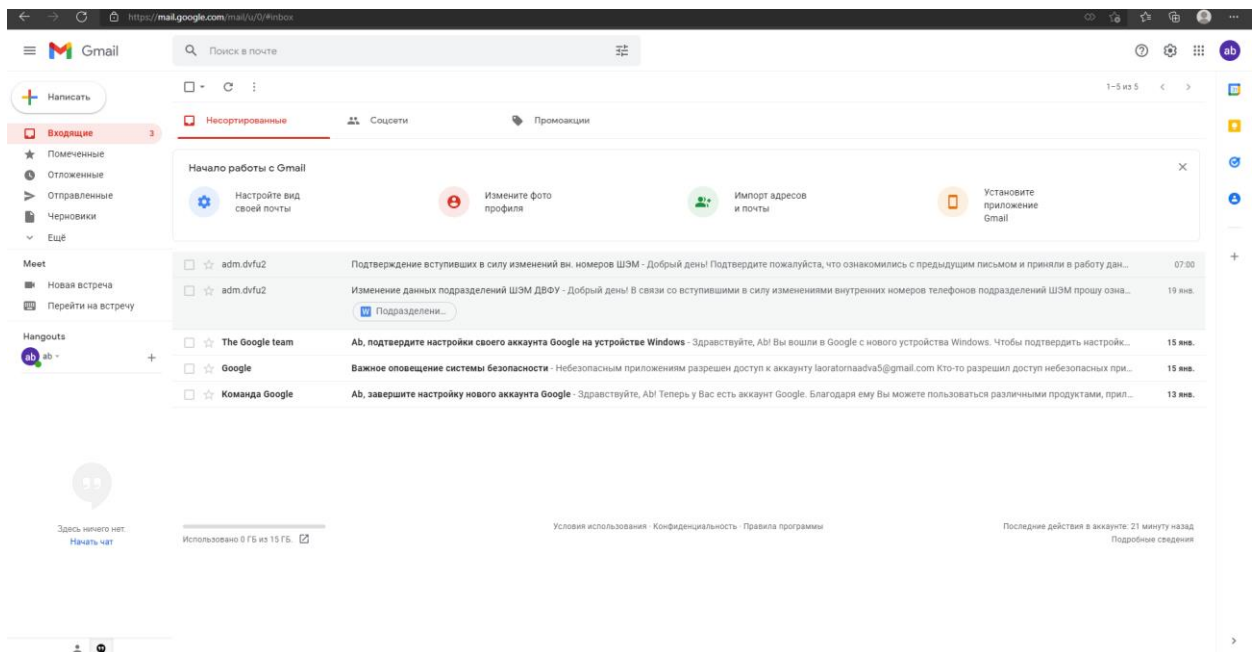
Главный менеджер

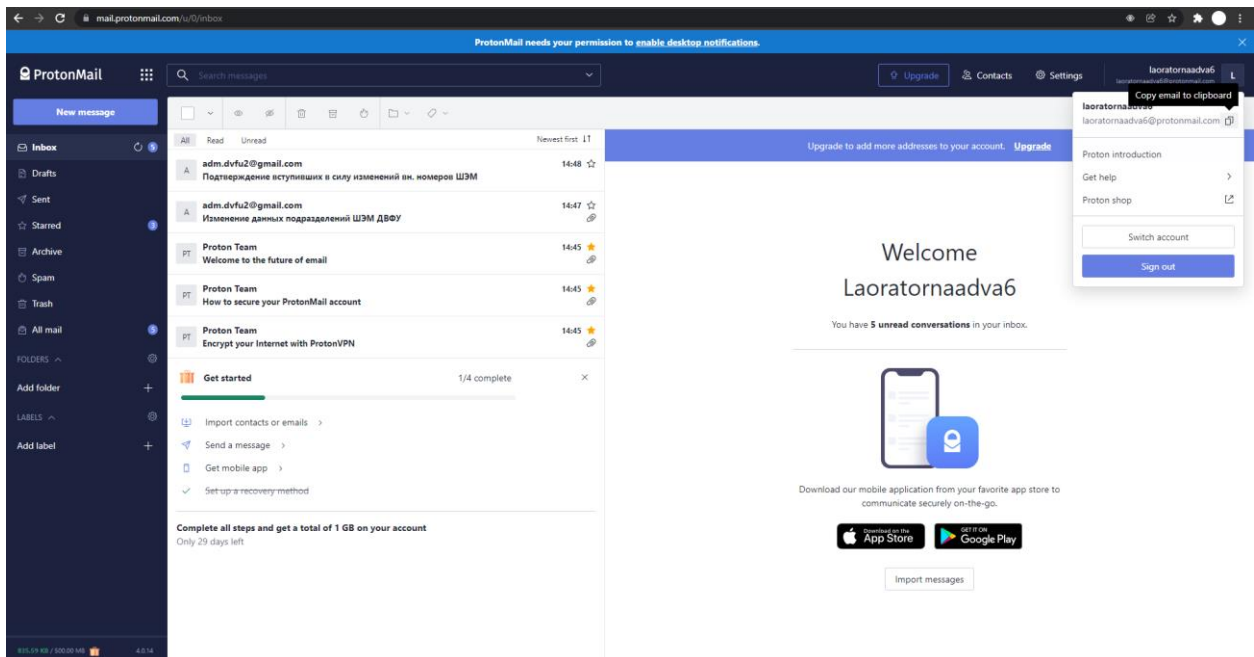
Административный отдел

Школа экономики и менеджмента

[Ответить](#)

[Переслать](#)





Результат открытия файла:

test\_user1  
(администратор)

Сведения

Документы

Инциденты

Настройки

Выйти

Версия 1.1.3009a

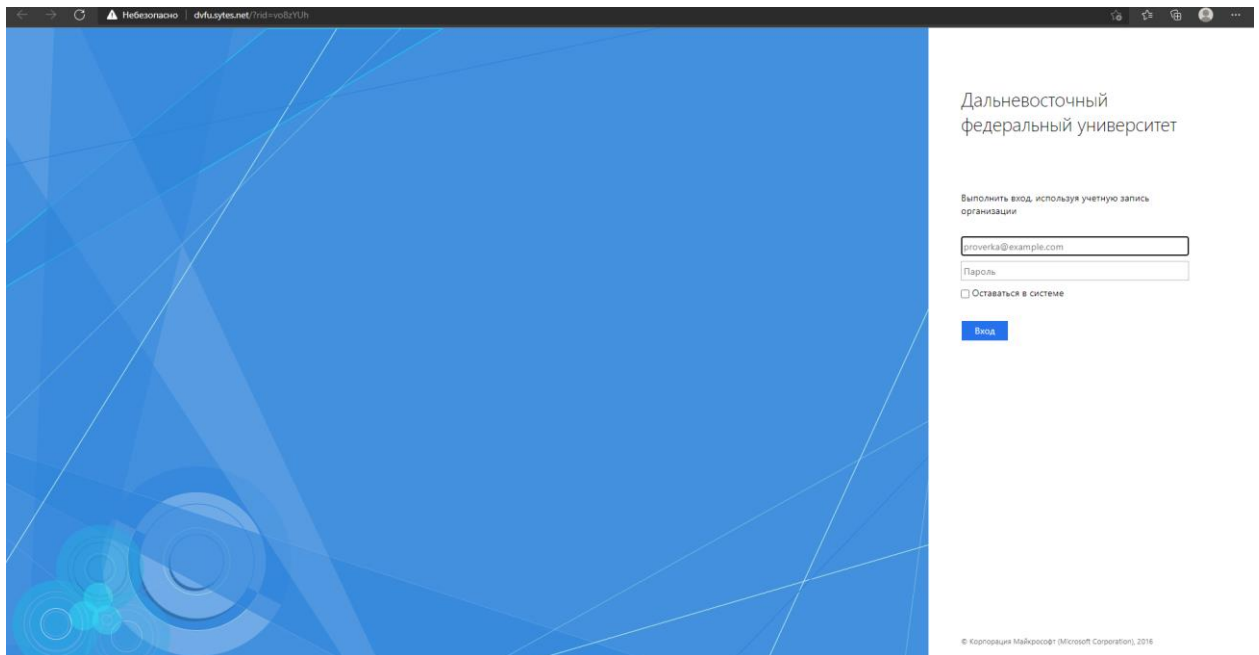
Инциденты

Количество записей: 10

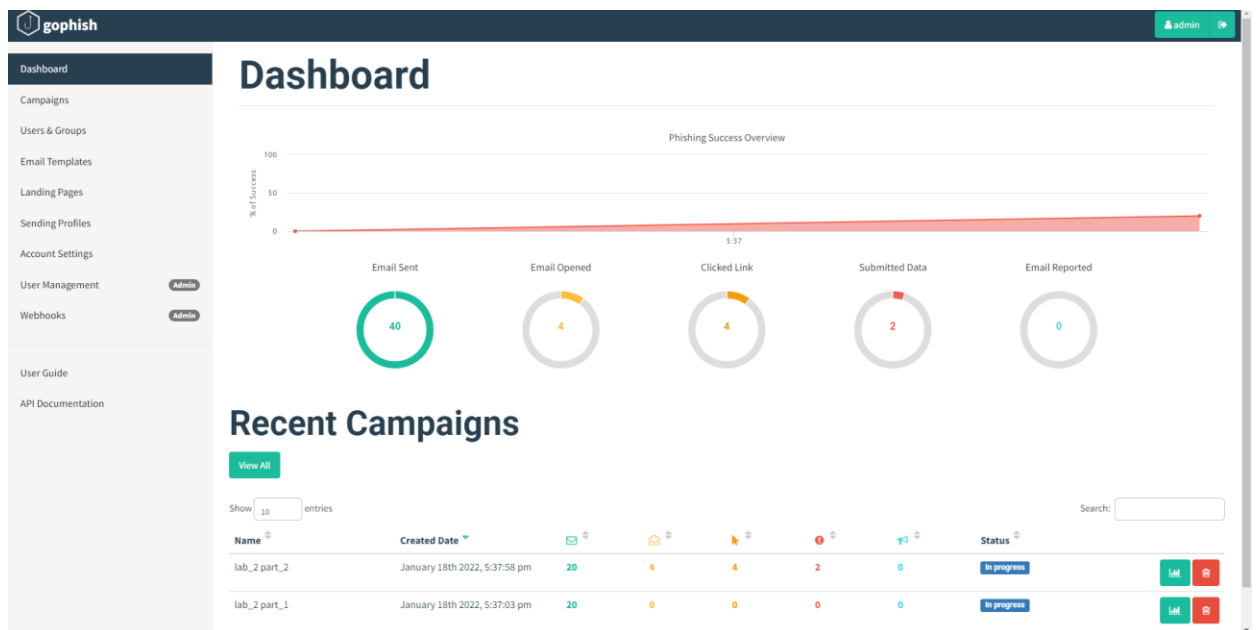
Фильтр:

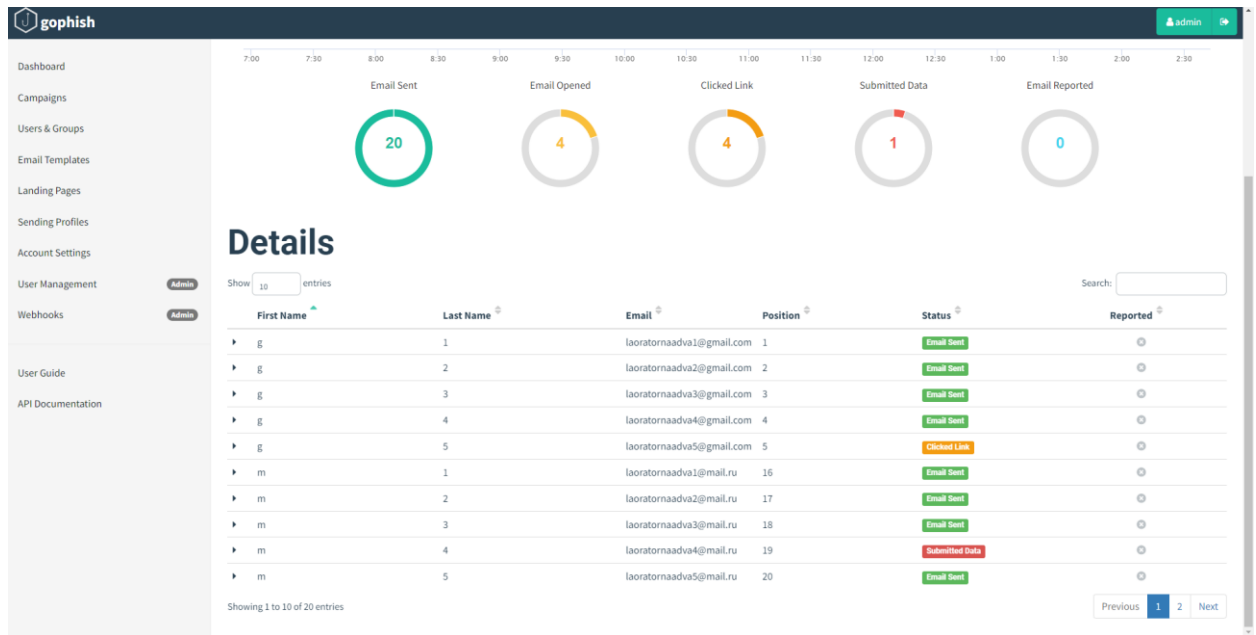
Дата и время	Метка документа	IP	User agent	Страна	Город	Координаты
2022-01-20 14:26:01	q5vj6k3r8h1roobryp4bimclpx3	95.154.66.37	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16)	Russia	Vladivostok	43.1056 с.ш. 131.8735 в.д.
2022-01-16 16:22:41	q5vj6k3r8h1roobryp4bimclpx3	95.154.66.37	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16)	Russia	Vladivostok	43.1056 с.ш. 131.8735 в.д.
2022-01-16 16:15:14	q5vj6k3r8h1roobryp4bimclpx3	95.154.66.37	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16)	Russia	Vladivostok	43.1056 с.ш. 131.8735 в.д.

Так выглядит фишинговый сайт:



Результат рассылки:





Полученные аутентификационные данные, введенные на фишинговом сайте:

