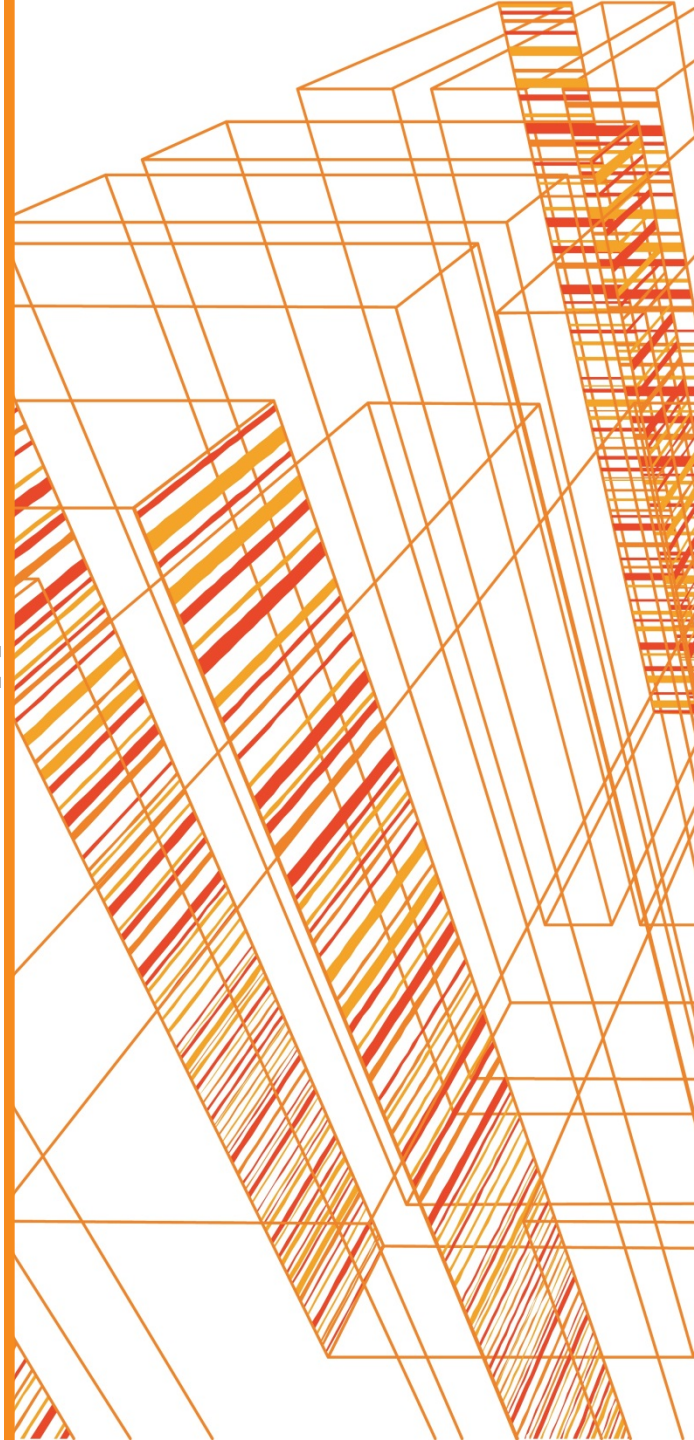
ЕВРАЗ
мы делаем мир сильнее

Информационная безопасность: новые риски — эффективные решения

Повышение осведомлённости пользователей с помощью учебного фишинга

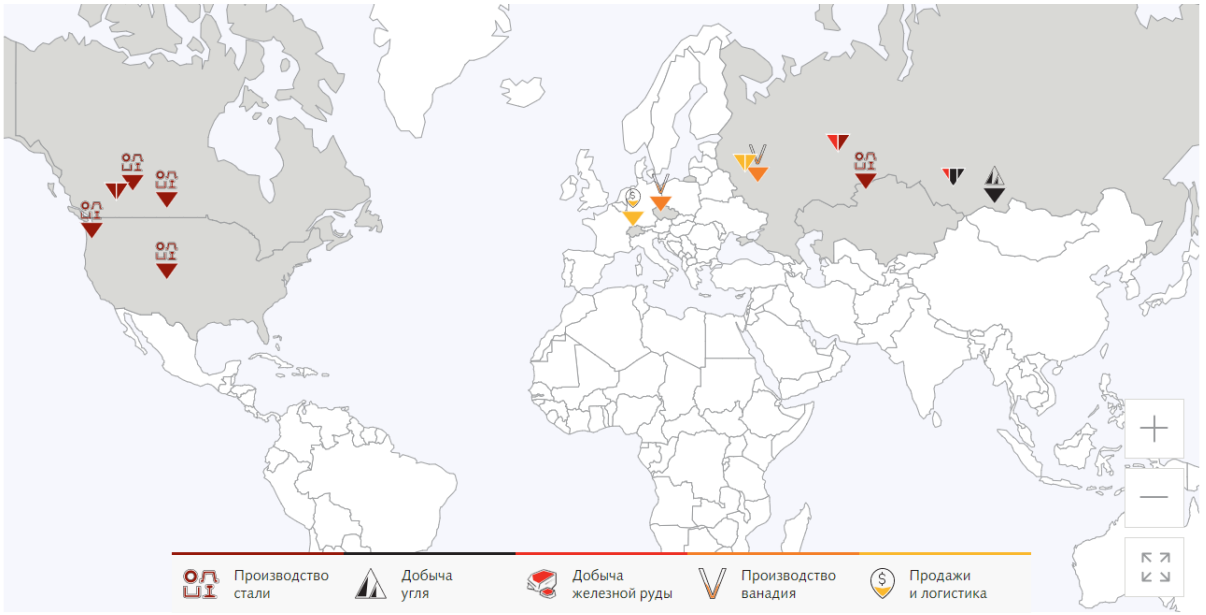
Нуйкин Андрей
ЕВРАЗ



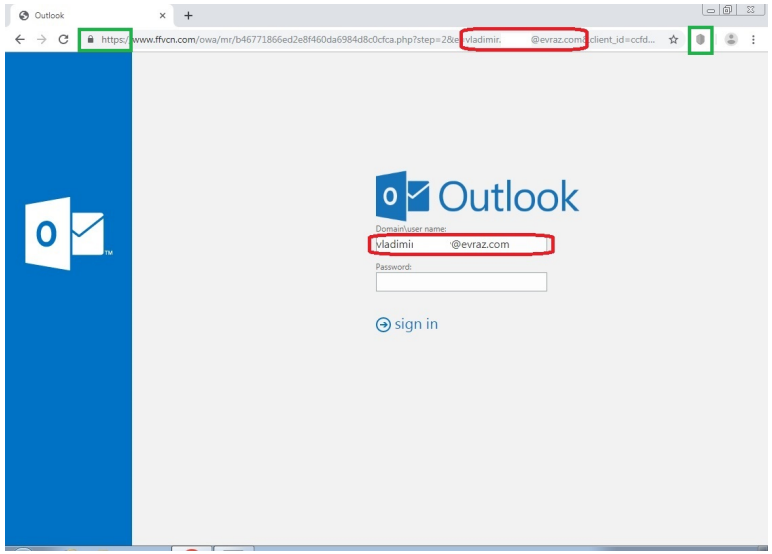
ЕВРАЗ

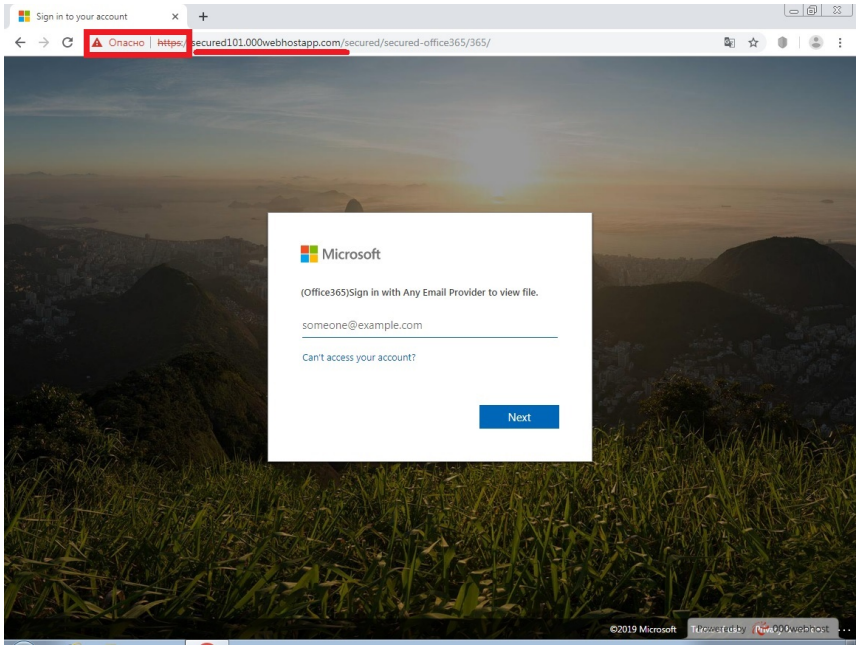
ГЛОБАЛЬНАЯ ГОРНО-МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

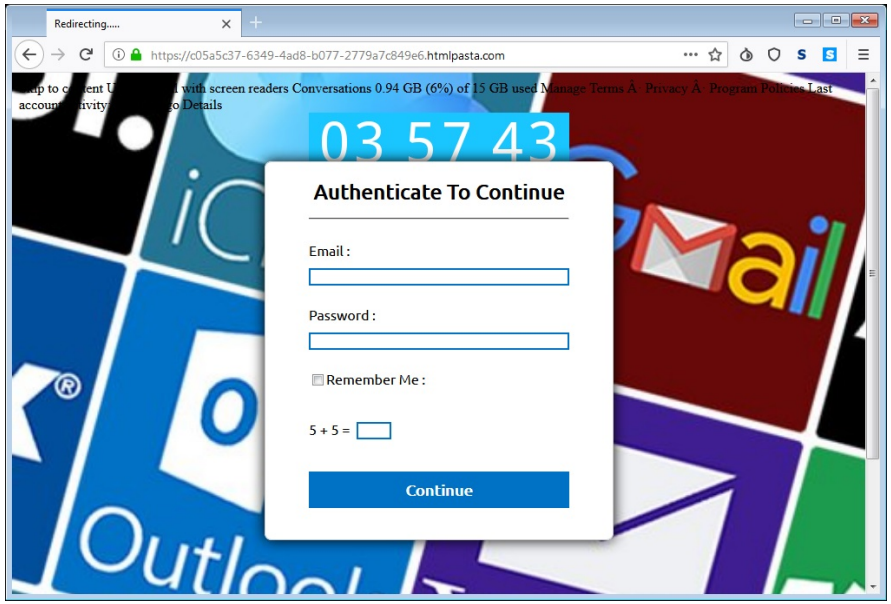
ЕВРАЗ является вертикально-интегрированной металлургической и горнодобывающей компанией с активами в России, США, Канаде и Казахстане. Компания входит в число крупнейших производителей стали в мире. Собственная база железной руды и коксующегося угля практически полностью обеспечивает внутренние потребности ЕВРАЗа. Компания входит в ведущий индекс Лондонской Фондовой Биржи FTSE-100.

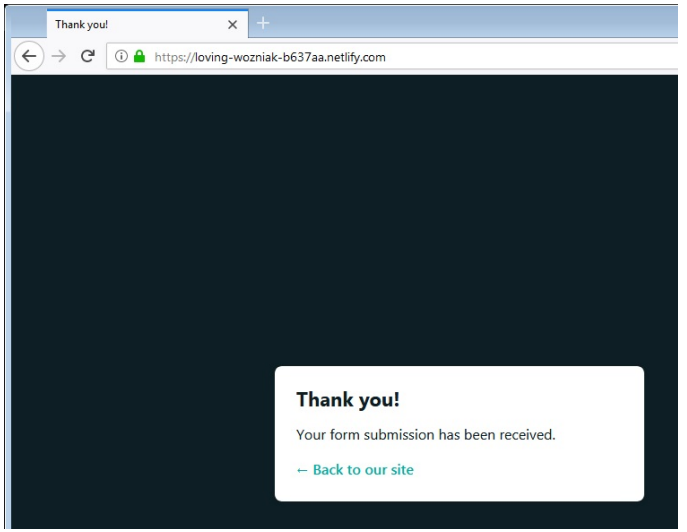


Предпосылки для проведений учений



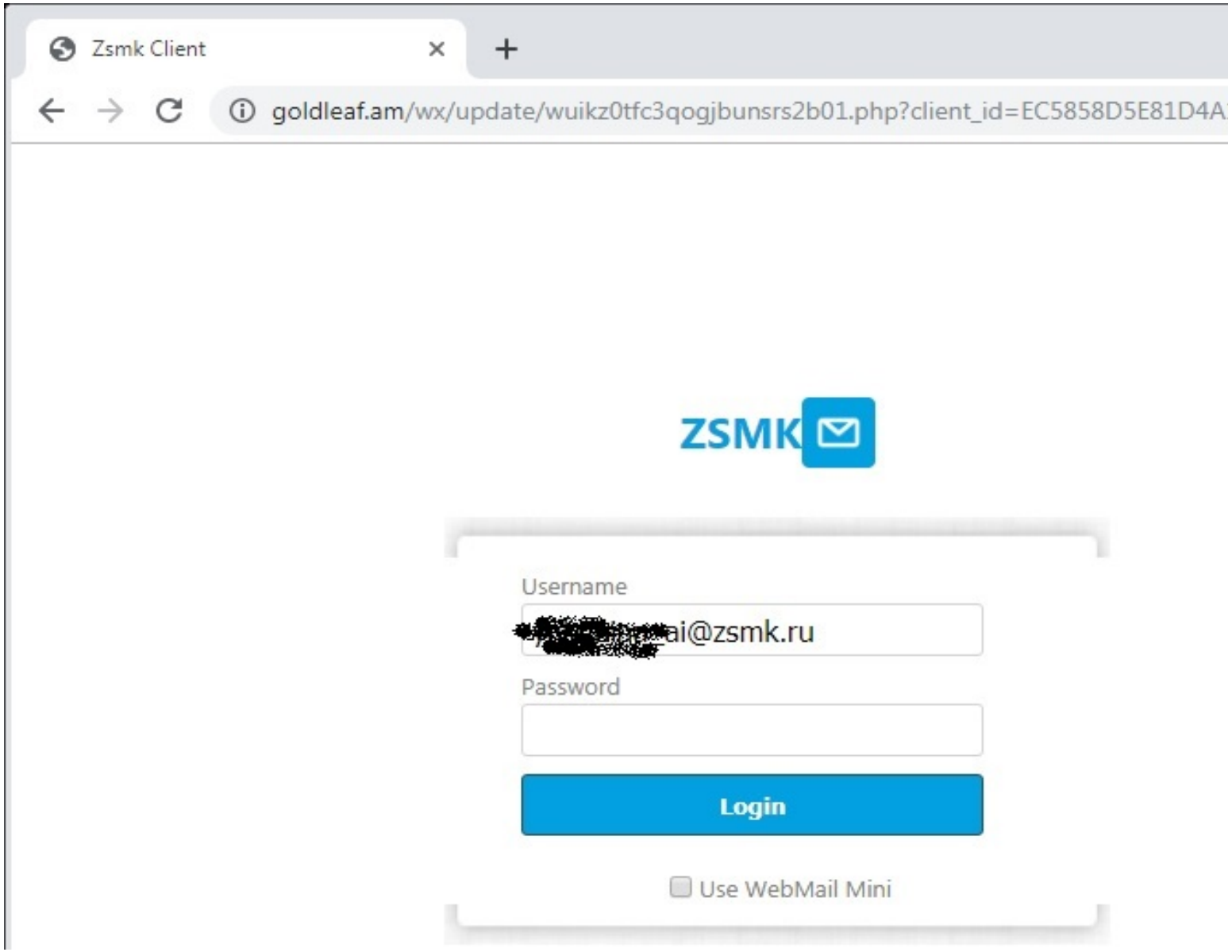






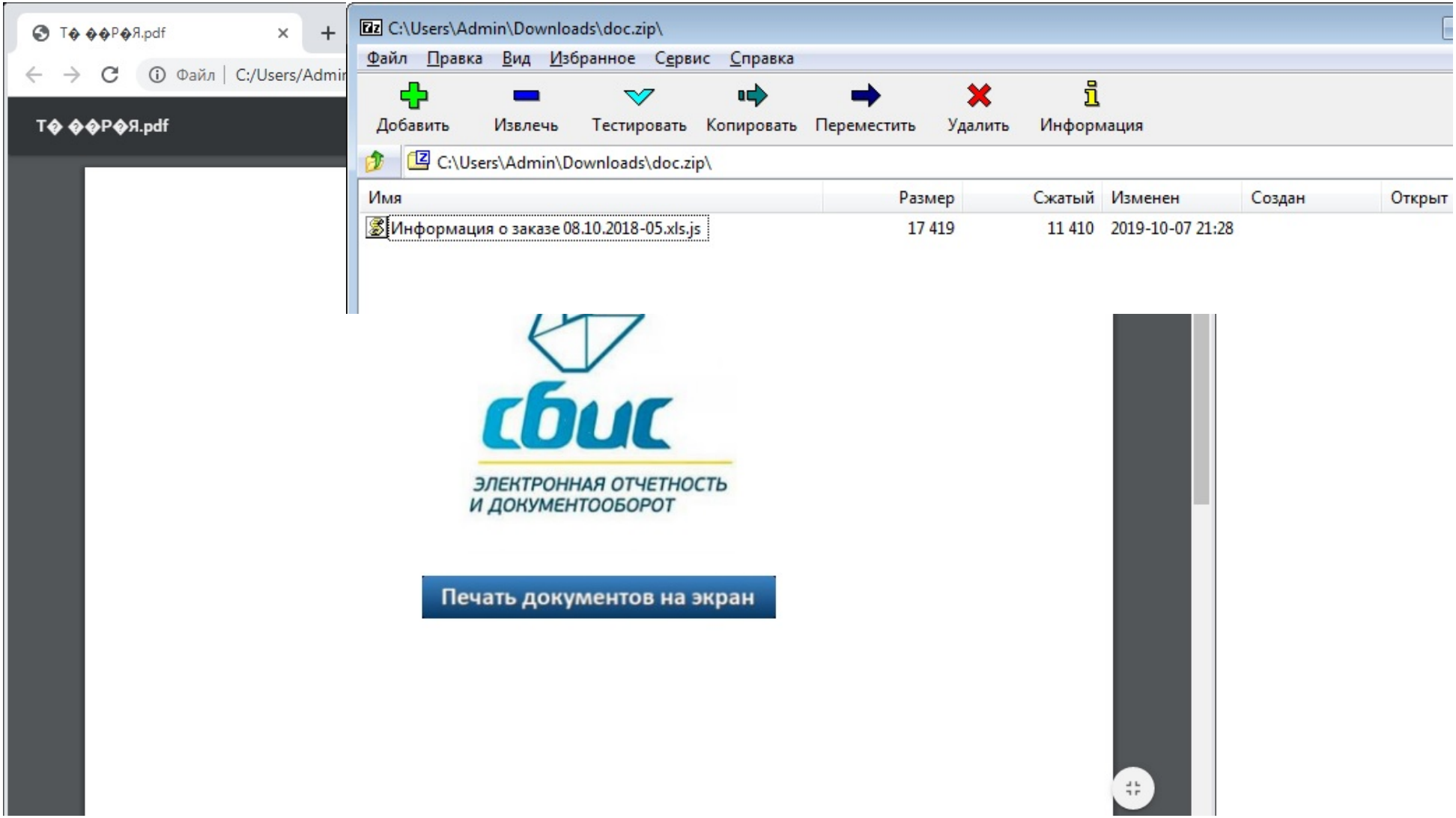
ЕВРАЗ

Предпосылки для проведений учений



ЕВРАЗ

Предпосылки для проведений учений

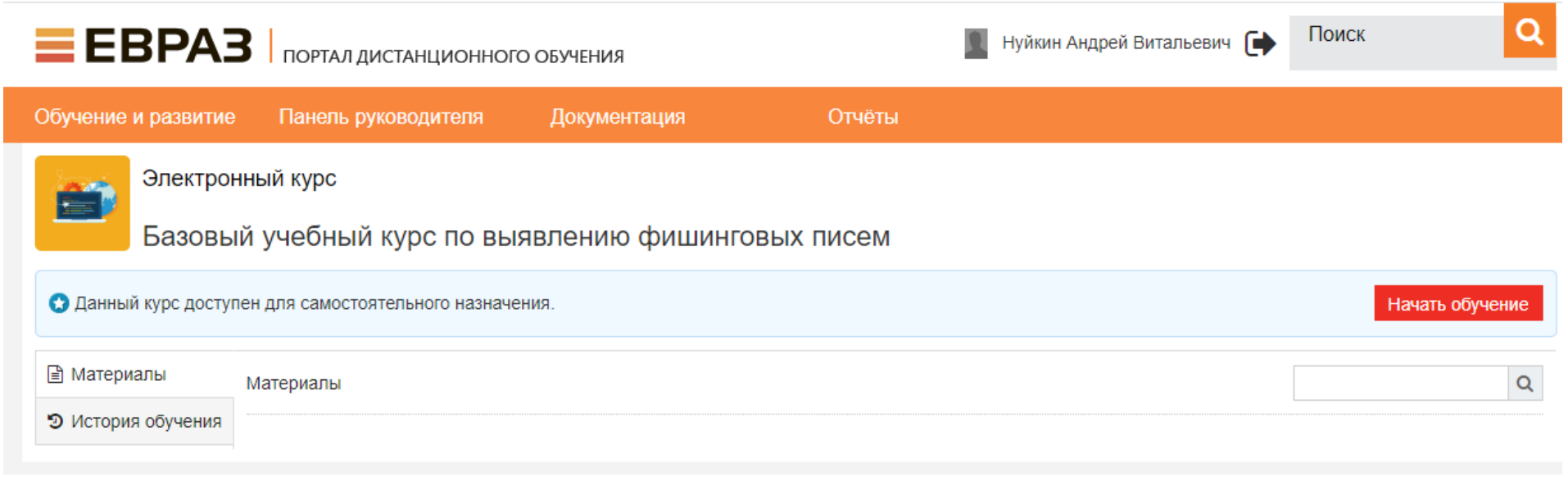


ЕВРАЗ

Определение цели

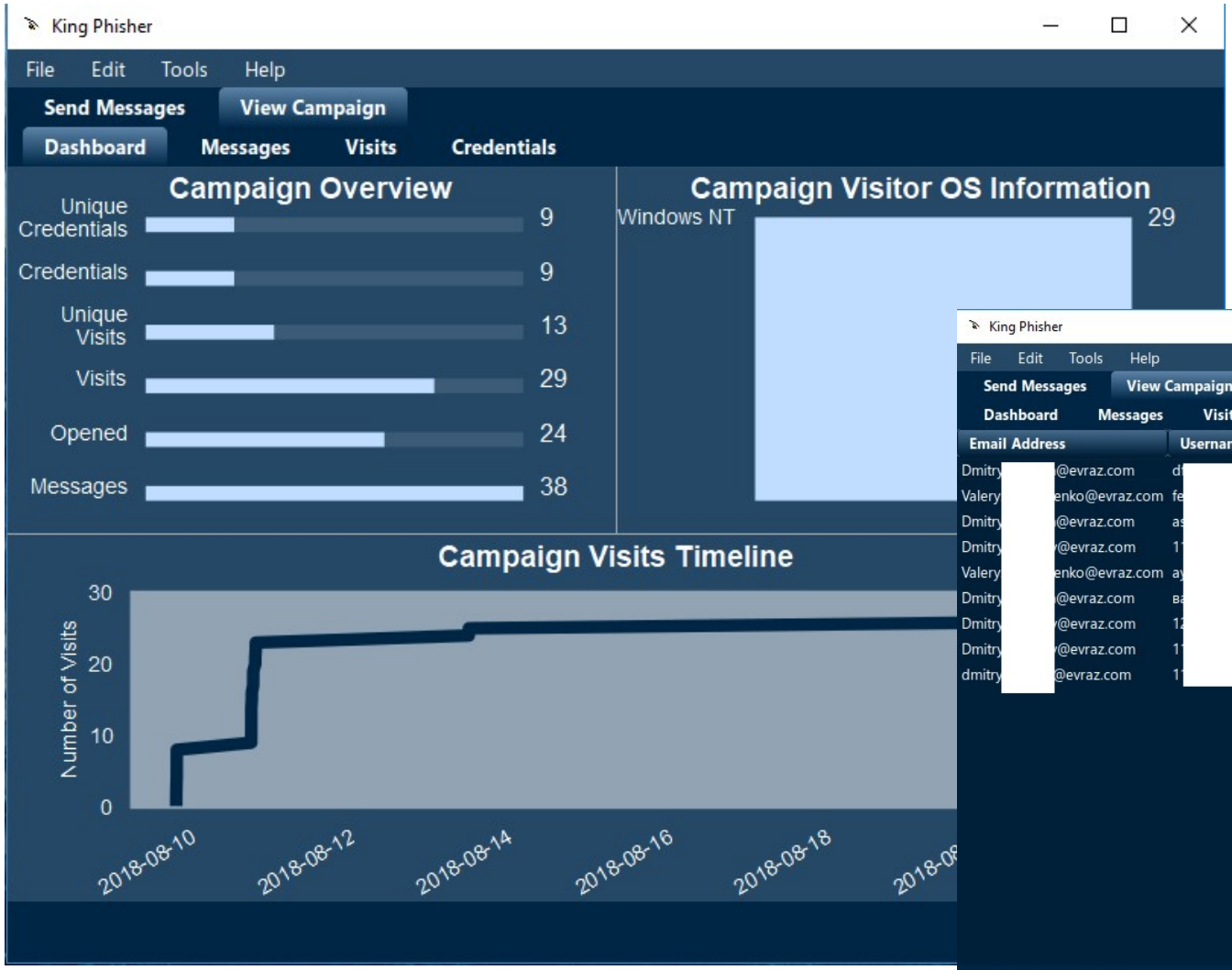
Цель:

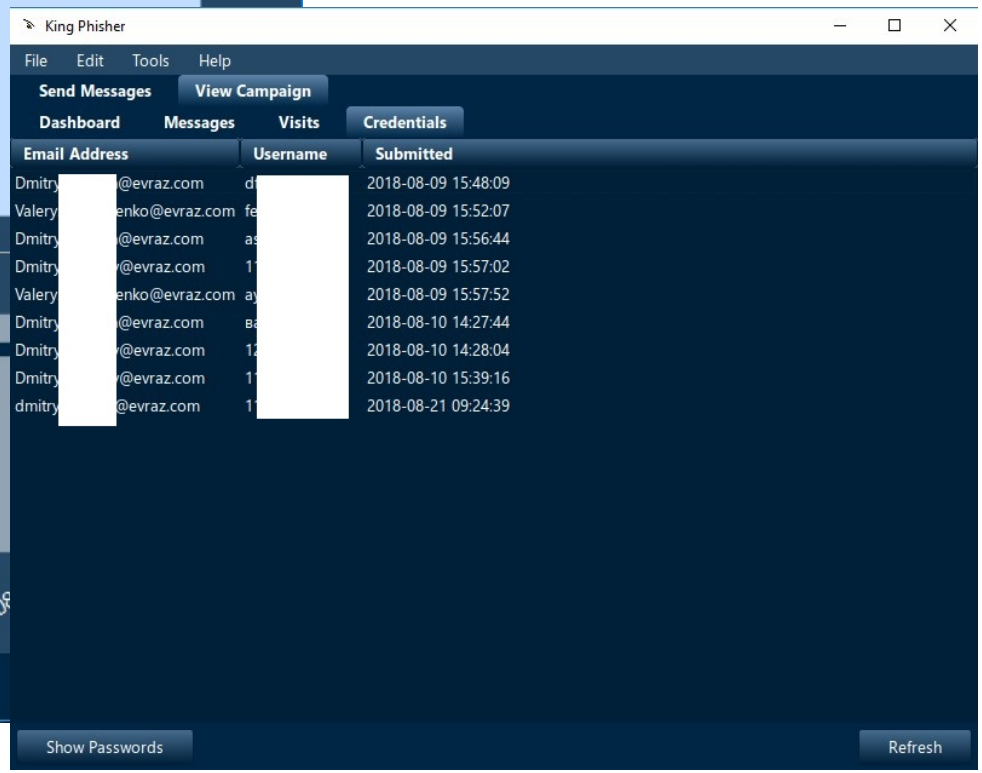
1. Оценить вероятность утечки учетных данных от корпоративных учетных записей.
2. Повысить степень вовлеченности пользователей в процесс противодействия фишинговым атакам.
3. Повысить уровень осведомленности пользователей.
4. Оценить результаты мероприятий по обучению.



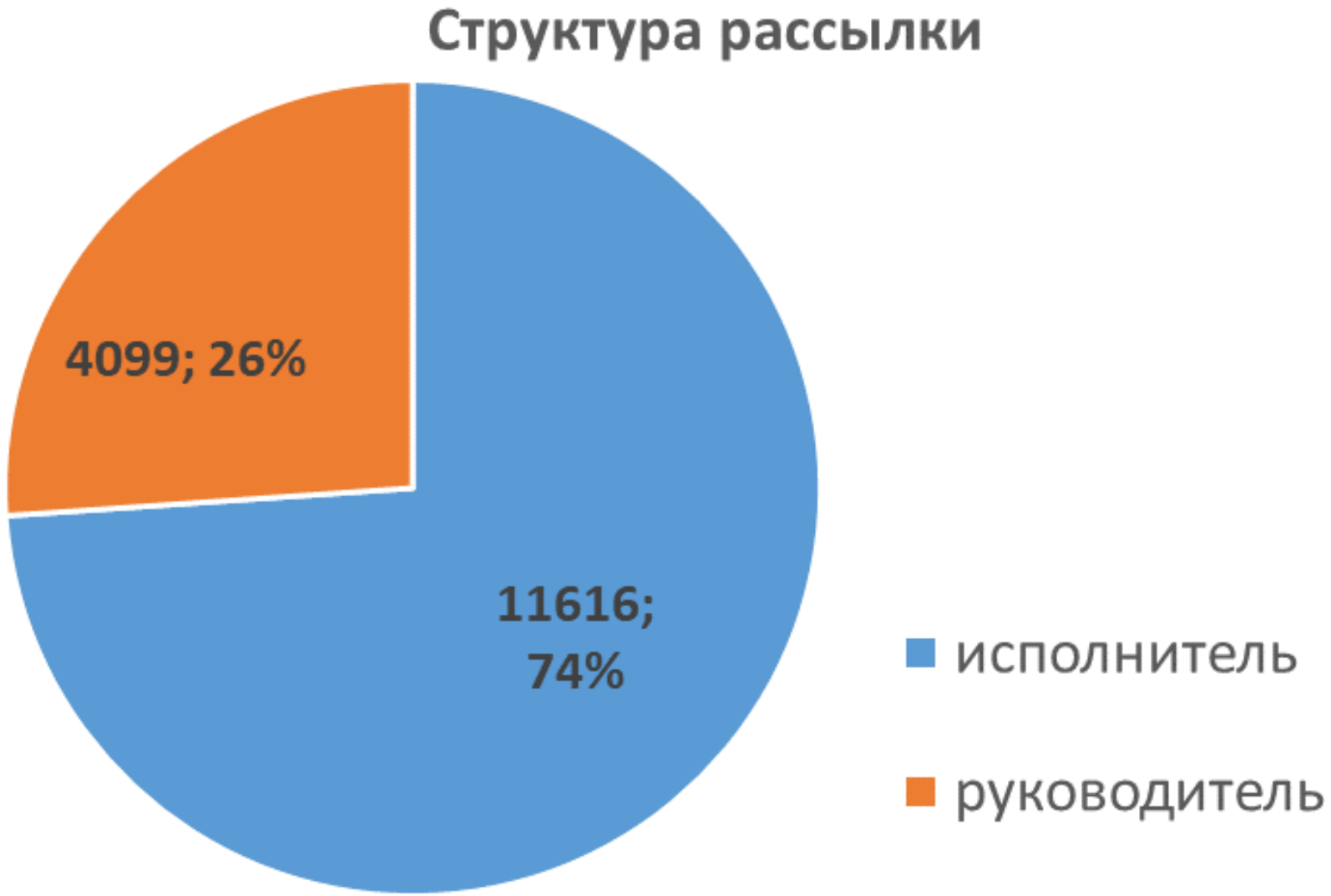
ЕВРАЗ

Подготовка


King Phisher
File Edit Tools Help
Send Messages View Campaign
Dashboard Messages Visits Credentials
Campaign Overview
Unique Credentials 9
Credentials 9
Unique Visits 13
Visits 29
Opened 24
Messages 38
Campaign Visitor OS Information
Windows NT 29
Campaign Visits Timeline
Number of Visits
30
20
10
0
2018-08-10
2018-08-12
2018-08-14
2018-08-16
2018-08-18

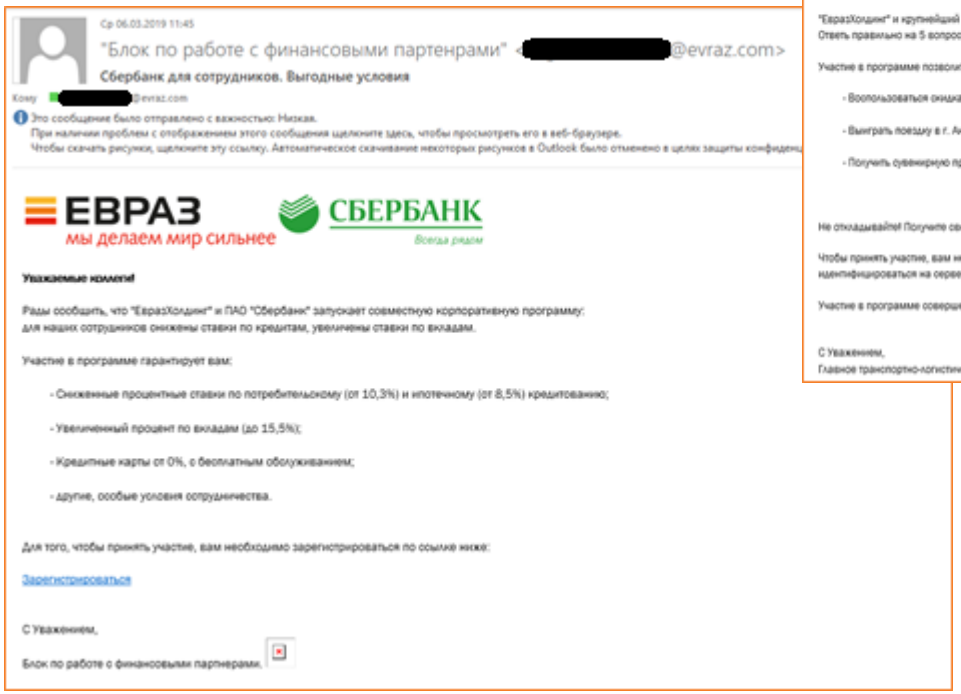

King Phisher
File Edit Tools Help
Send Messages View Campaign
Dashboard Messages Visits Credentials
Email Address
Username
Submitted
2018-08-09 15:48:09
2018-08-09 15:52:07
2018-08-09 15:56:44
2018-08-09 15:57:02
2018-08-09 15:57:52
2018-08-10 14:27:44
2018-08-10 14:28:04
2018-08-10 15:39:16
2018-08-21 09:24:39
Show Passwords
Refresh

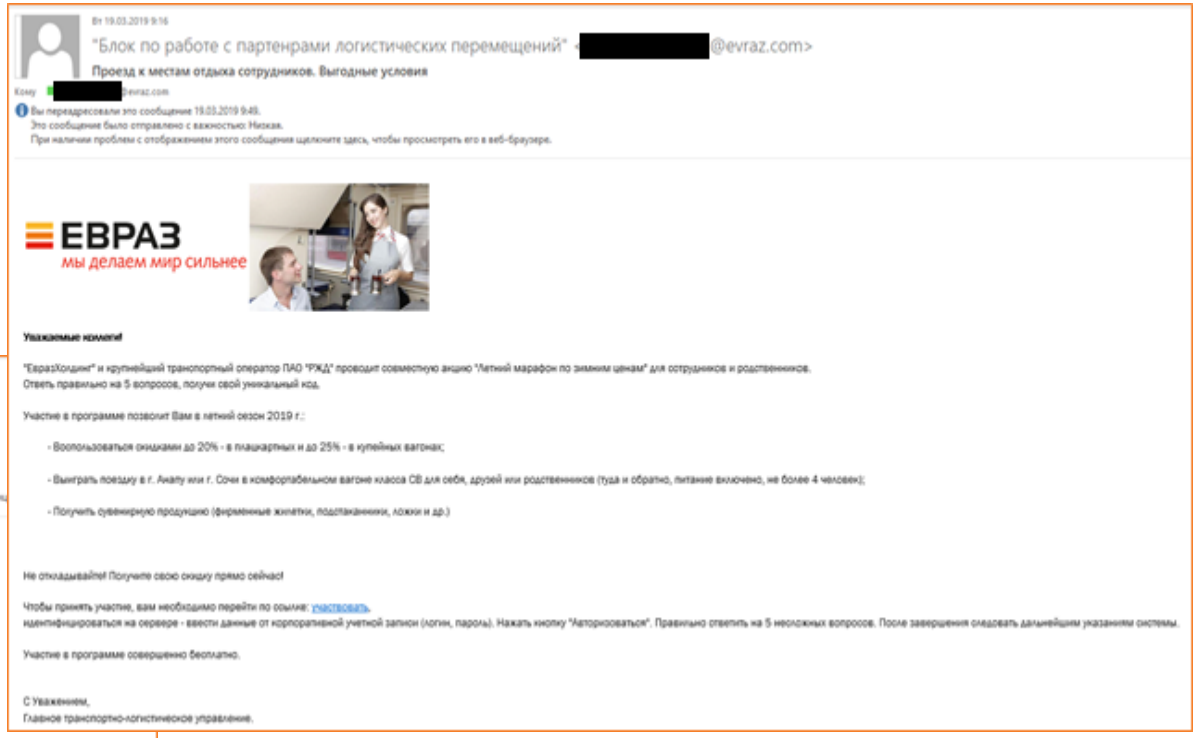
Масштабы охвата

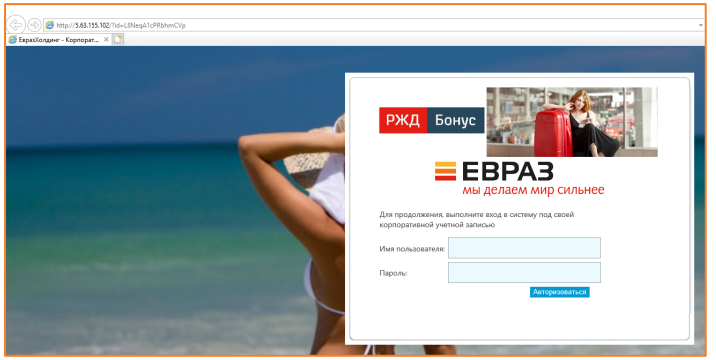


Первый этап – весна 2019

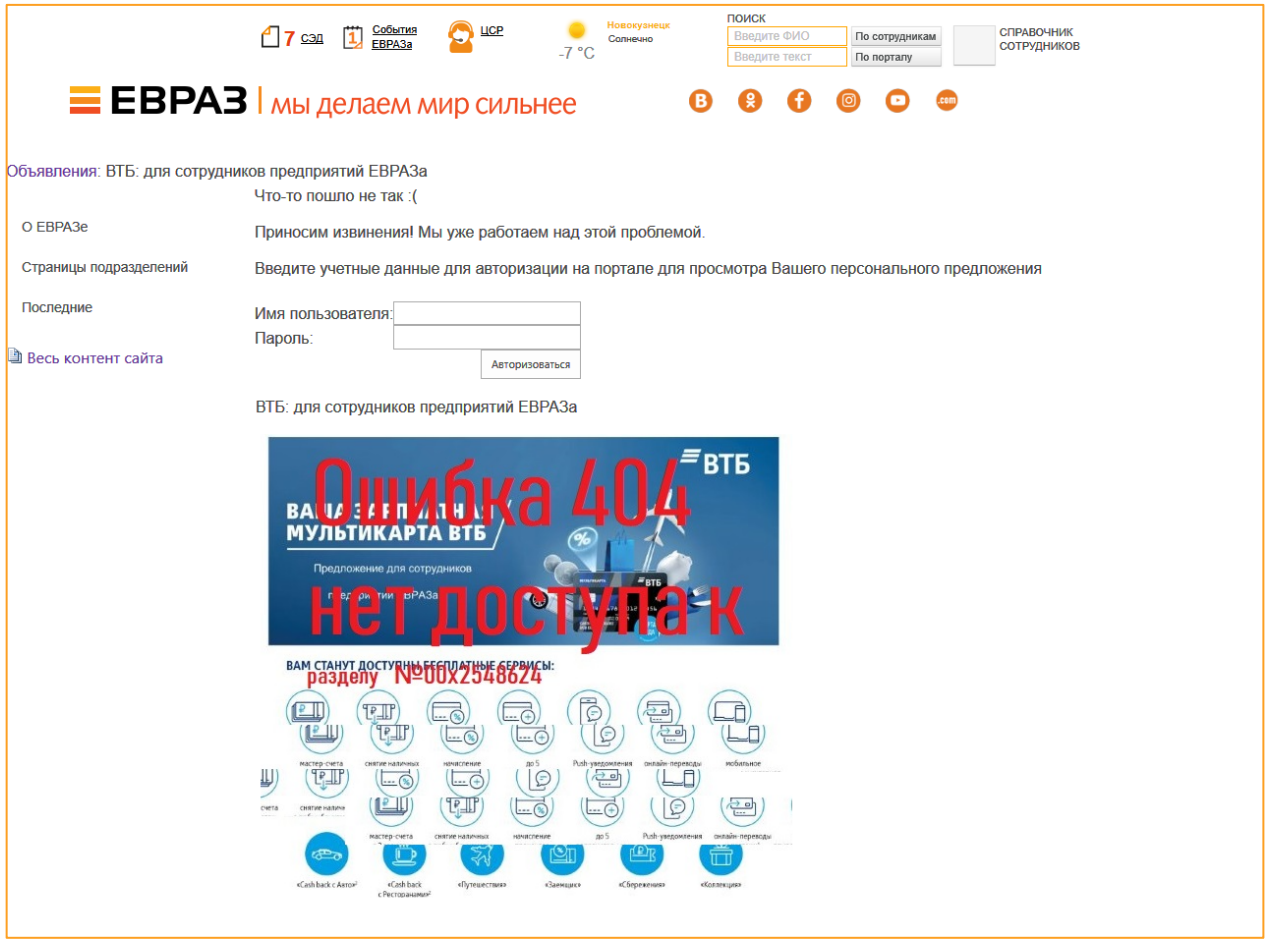
Результат 20.05.2019:
Писем отправлено – 12774
Сообщили о фишинге – 103
Передали свои данные - 417







Второй этап – осень 2019



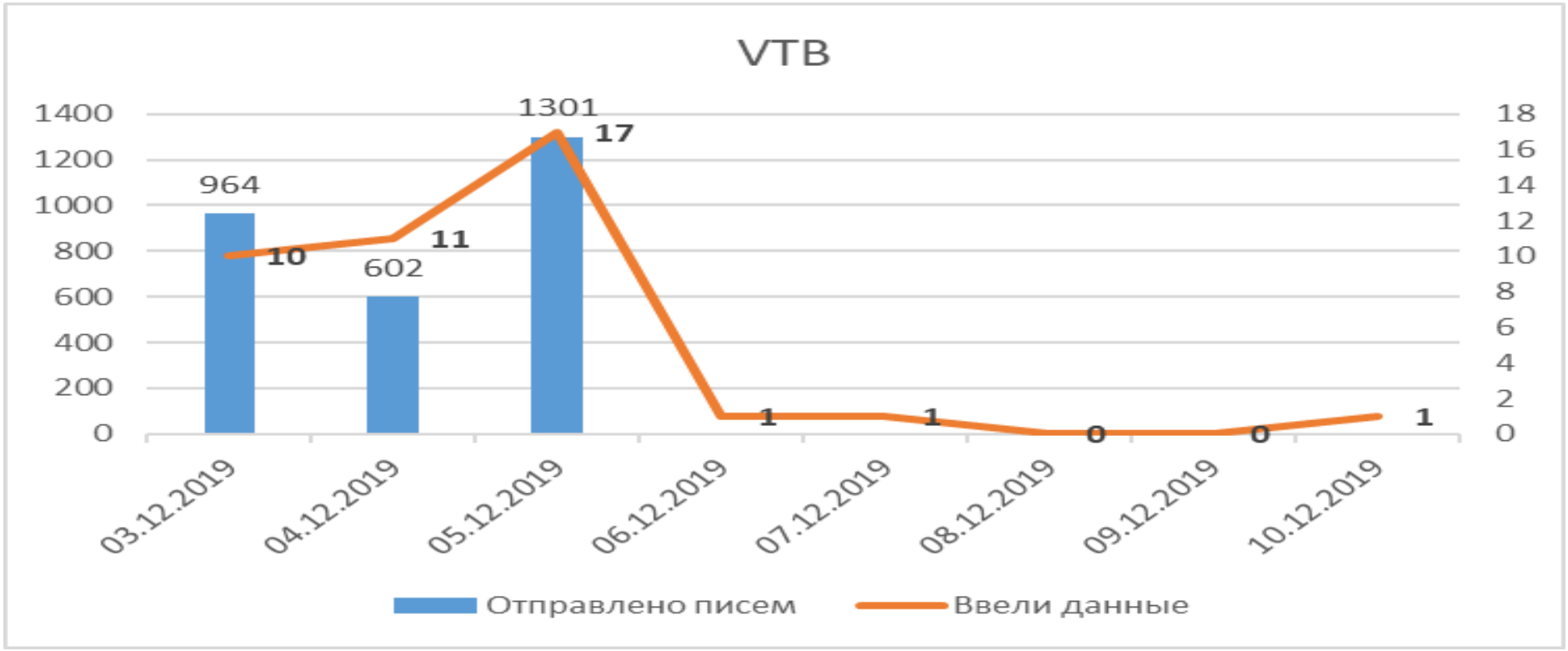
ВТБ

ЕВРАЗ

Результаты по теме «ВТБ»

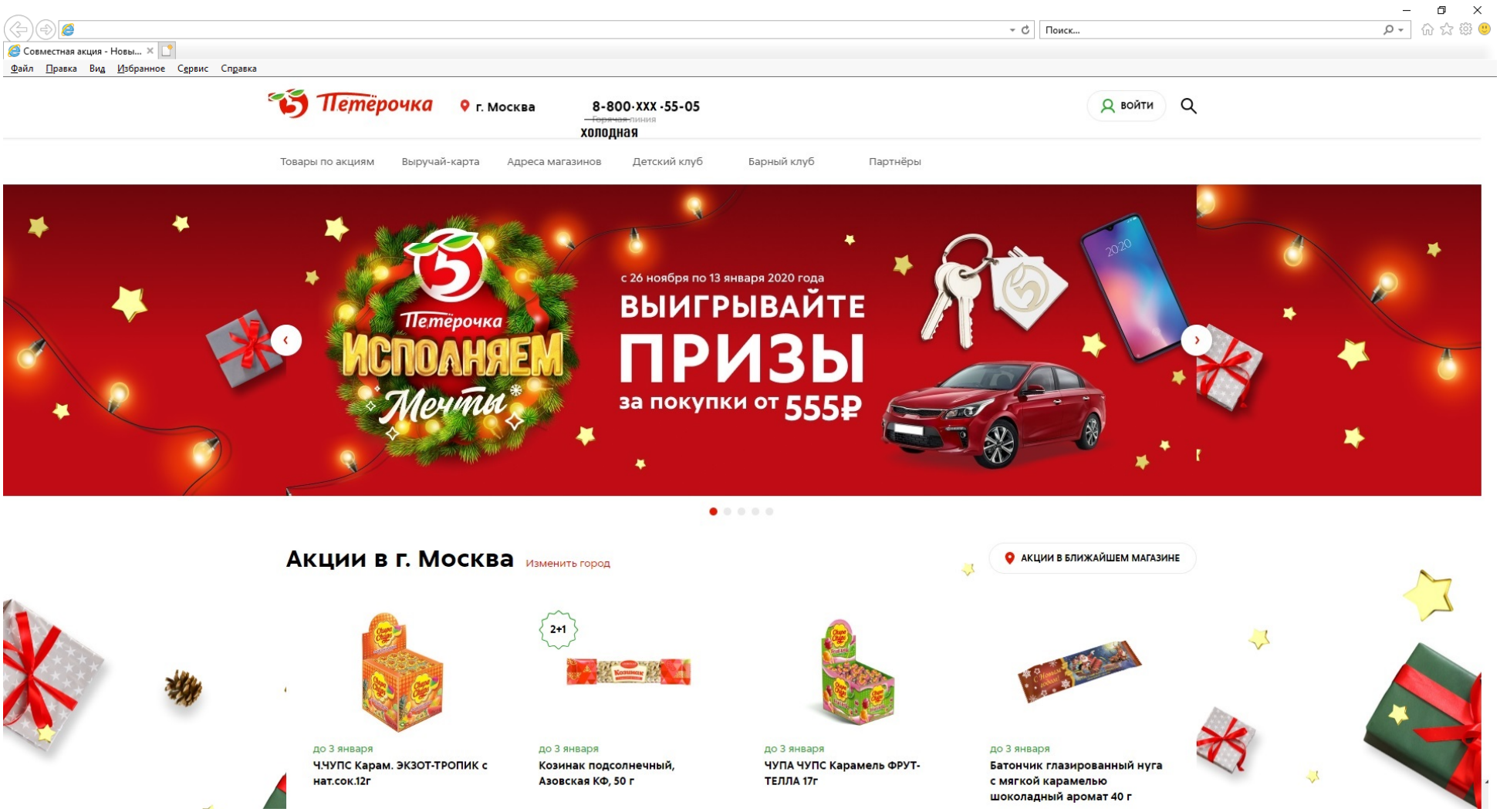
Количество откликов в Техподдержку:
3,9 откликов на 100 разосланных писем

Результативность темы:
1,4 скомпрометированных учетных записей на 100 писем



ЕВРАЗ

Тема Пятерочка



ЕВРАЗ

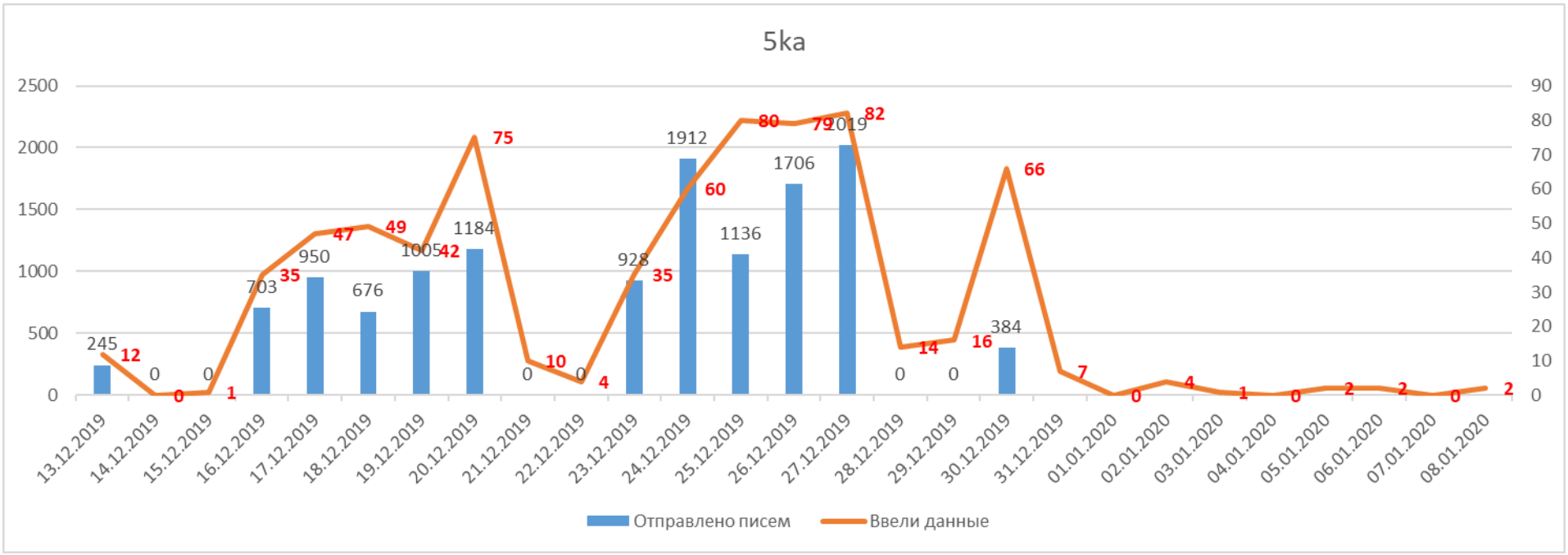
Результаты по теме «Пятерочка»

Количество откликов в Техподдержку:

3,4 откликов на 100 разосланных писем

Результативность темы:

5,6 скомпрометированных учетных записей на 100 писем



ЕВРАЗ

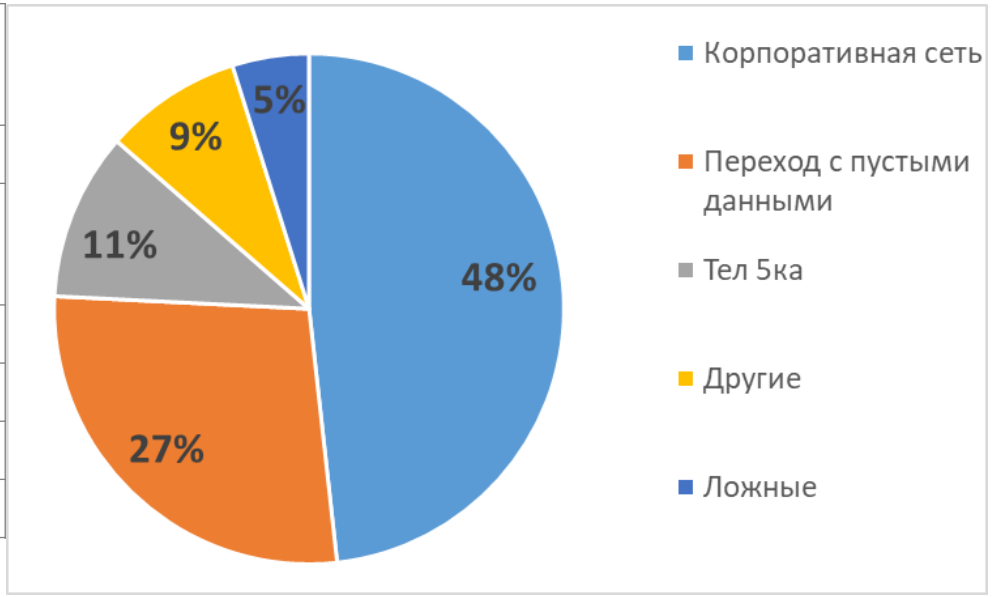
Какие данные вводили пользователи

1111 перешедших по ссылке сделали в среднем по 3,7 попытки ввести данные

Всего данные вводили 4087 раз.

Структура вводимых данных

Принадлежность данных	Кол-во	%
Корпоративная сеть	536	48%
Переход с пустыми данными	306	28%
Тел 5ка	118	11%
Другие	97	9%
Ложные	54	5%
Итого	1111	100%



ЕВРАЗ

Сравнение кампаний: июнь с декабрем 2019

Результаты сравнения приведены в таблице

Наименование	Июнь 2019		Декабрь 2019	
	Количество	% от отправленных	Кол-во	% от отправленных
Отправлено	12774		15715	
Перешли по ссылкам	1174	9,2%	1111	7,1%
из них по QR коду	-	-	18	0,1%
Сообщили	103	0,8%	552	3,5%
Собрано данных	417	3,3%	661	4,2%
из них от УЗ Корп.сети	417	3,3%	353	2,2%
из них по QR коду	-	-	20	0,1%

Итоги

Цель, связанная с повышением вовлеченности пользователей в процесс противодействия фишинговым атакам достигнута.

Резюме:

1. Вероятность утечки логинов и паролей от корпоративных учетных записей 2,2%, для ее реализации требуется разослать большое количество писем.
2. Учитывая, что после начала рассылок первые заявки начинали приходить через 15 – 20 минут, то при быстрой реакции есть возможность заблокировать e-mail злоумышленников и их web-ресурсы.
3. Пользователи чувствительны к теме рассылки, если подобрать правильную тему, то эффективность фишинга значительно возрастает.
4. Работу по повышению уровня осведомленности пользователей необходимо проводить постоянно.

Вопросы?

Андрей Нуйкин
+7 916 124 6287
Andrey.nuykin@evraz.com