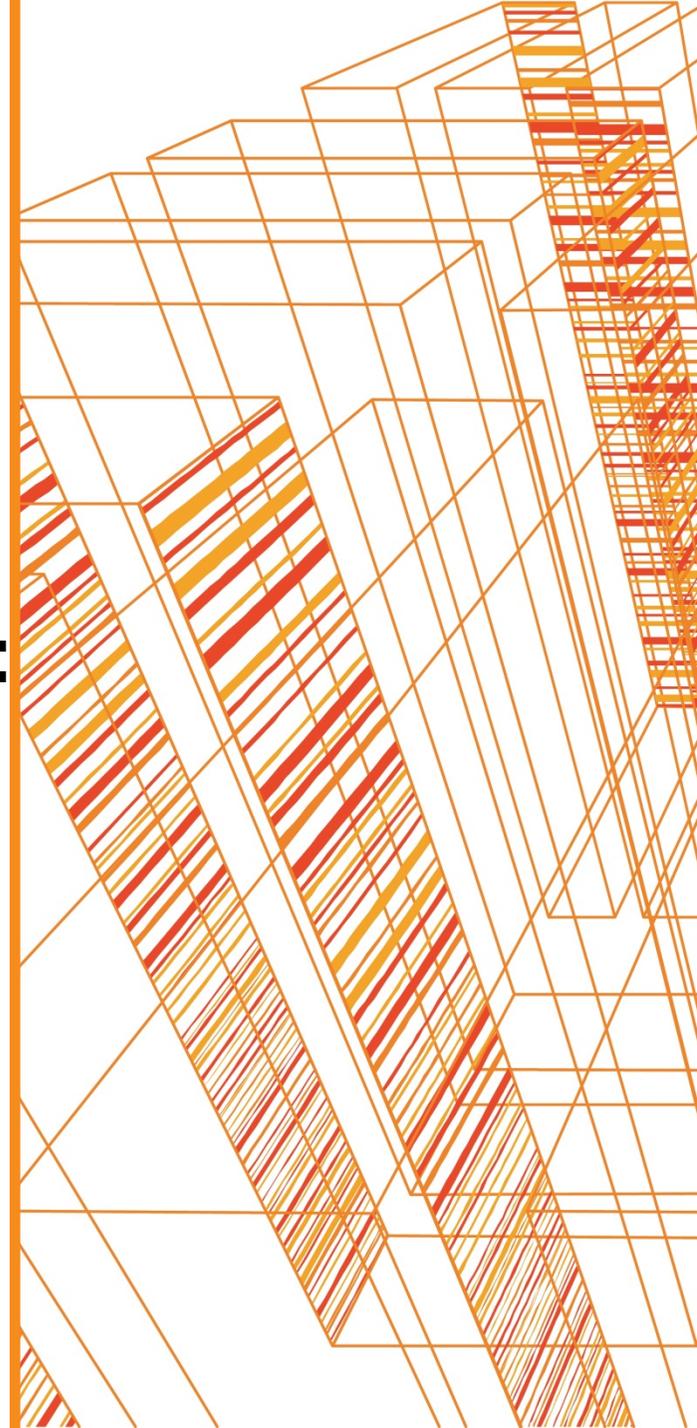


Информационная безопасность: новые риски — эффективные решения

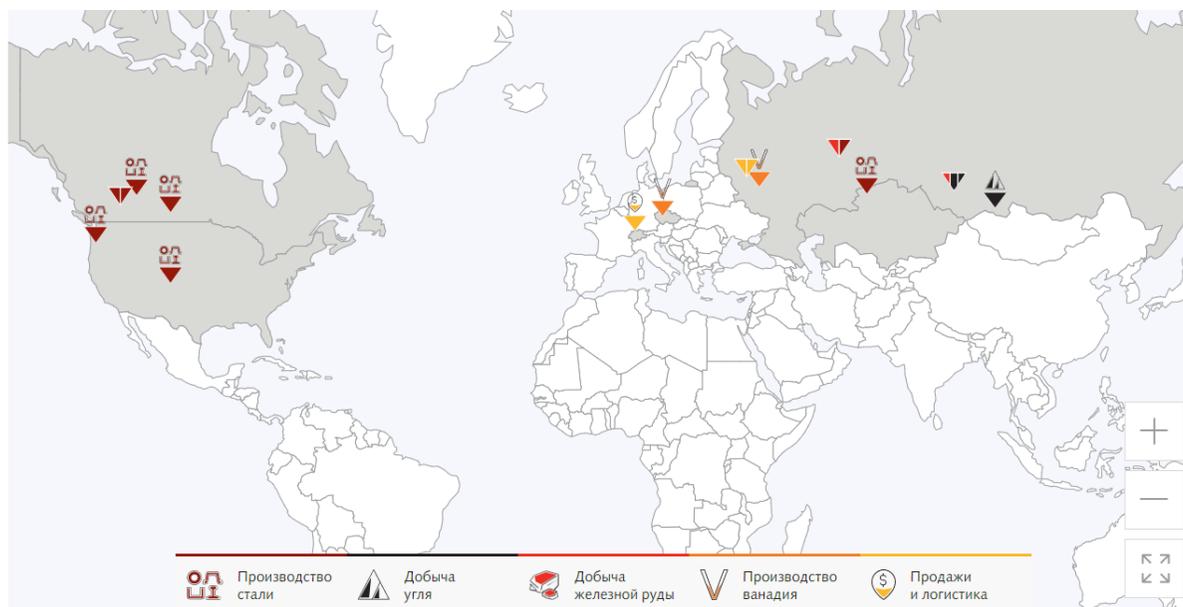
Повышение осведомлённости пользователей с помощью учебного фишинга

Нуйкин Андрей
ЕВРАЗ

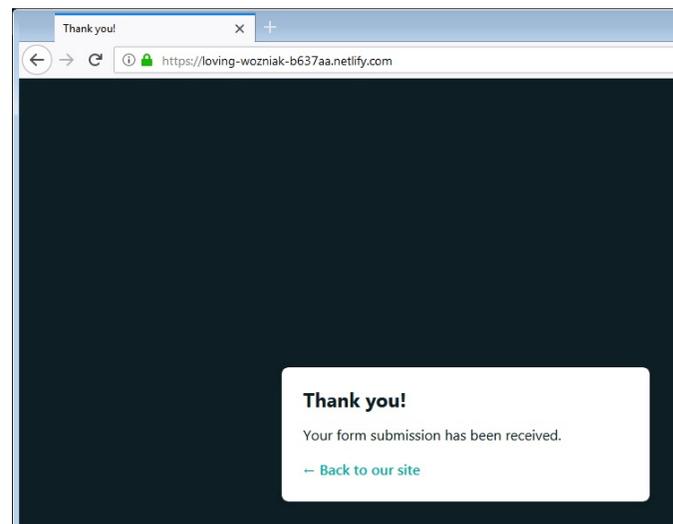
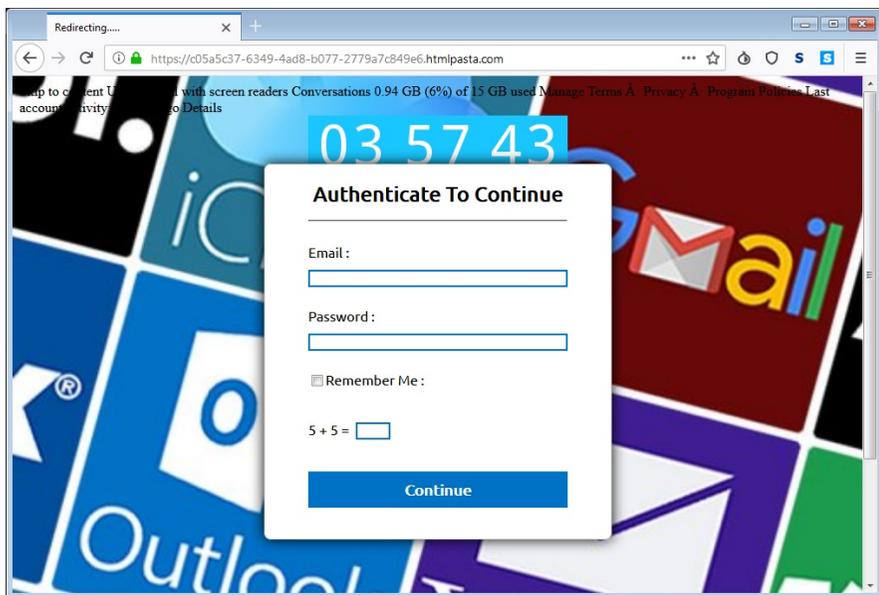
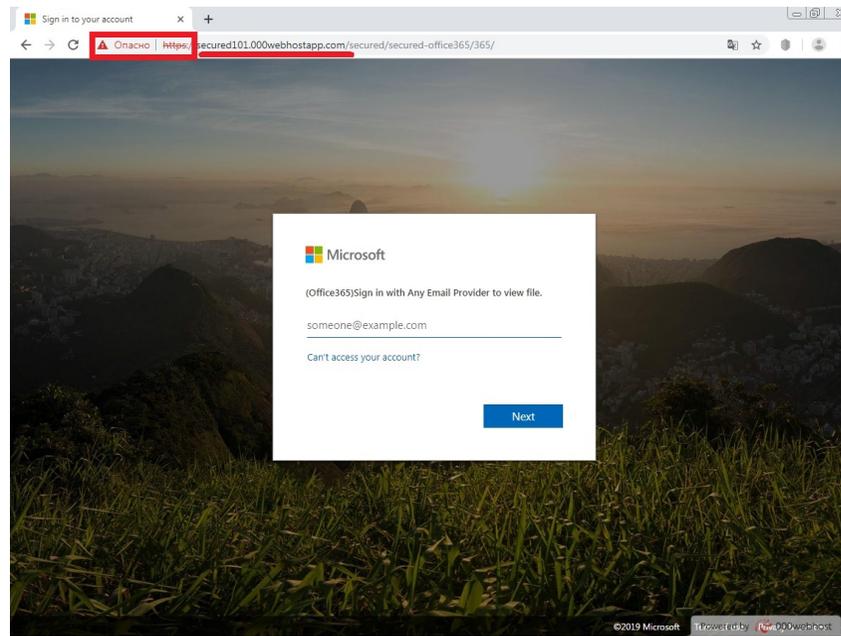
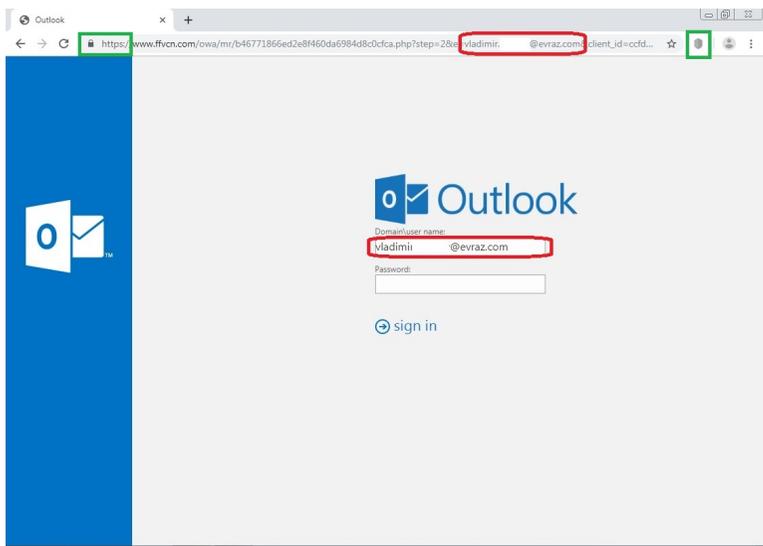


□ ГЛОБАЛЬНАЯ ГОРНО-МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

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 проведения учений



Предпосылки для проведения учений

Zsmk Client

goldleaf.am/wx/update/wuikz0tfc3qogjbunsrs2b01.php?client_id=EC5858D5E81D4A

ZSMK

Username

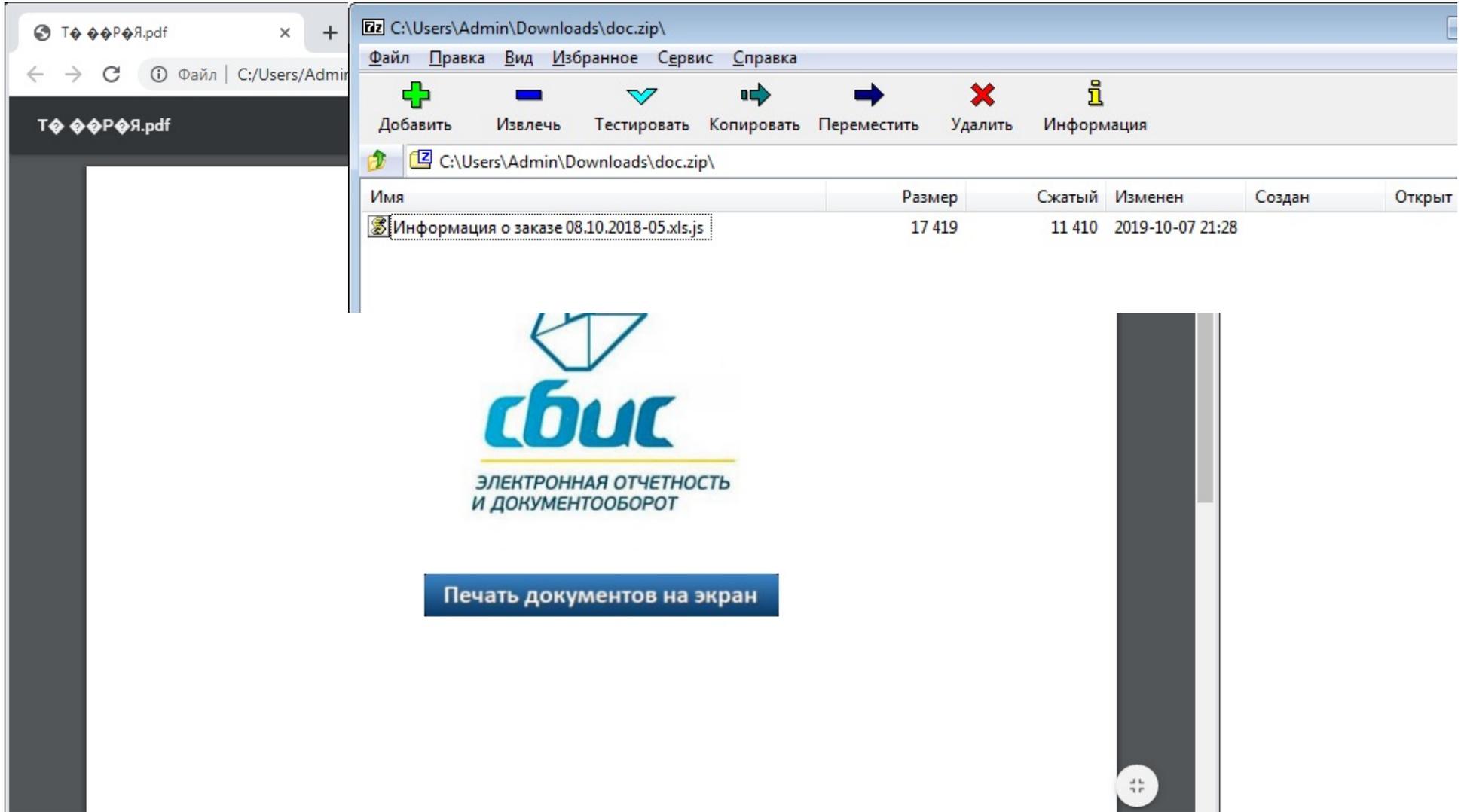
[Redacted]@zsmk.ru

Password

Login

Use WebMail Mini

Предпосылки для проведения учений



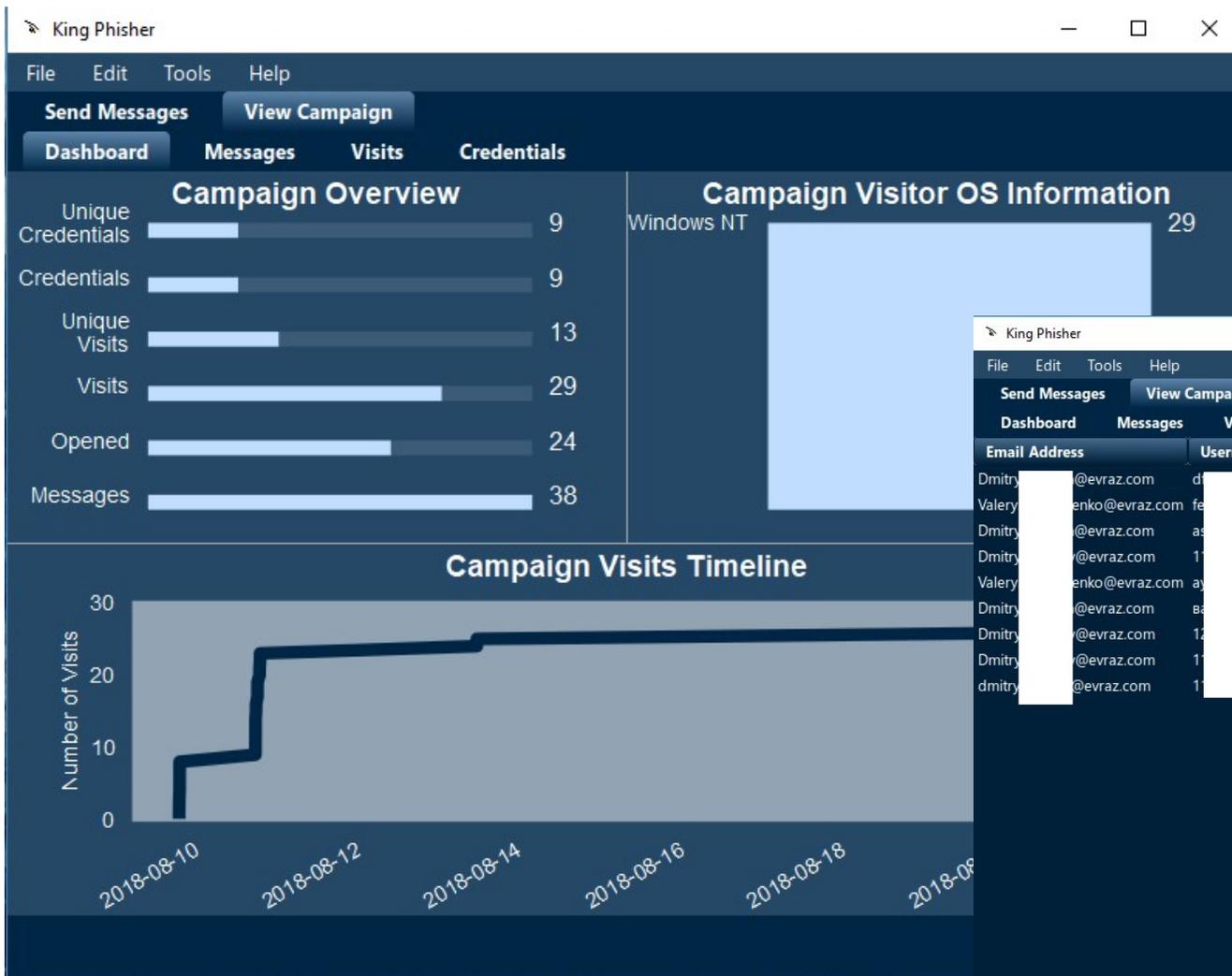
Определение цели

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.

The screenshot displays the EBRAZ portal interface. At the top left is the logo 'EBРАЗ' and the text 'ПОРТАЛ ДИСТАНЦИОННОГО ОБУЧЕНИЯ'. On the top right, there is a user profile 'Нуйкин Андрей Витальевич' and a search bar labeled 'Поиск'. Below the header is a navigation bar with links: 'Обучение и развитие', 'Панель руководителя', 'Документация', and 'Отчёты'. The main content area features a course card with a globe icon, titled 'Электронный курс' and 'Базовый учебный курс по выявлению фишинговых писем'. A light blue notification box states '★ Данный курс доступен для самостоятельного назначения.' with a red 'Начать обучение' button. Below the course card are tabs for 'Материалы' and 'История обучения', with 'Материалы' selected. A search bar is located to the right of the 'Материалы' tab.

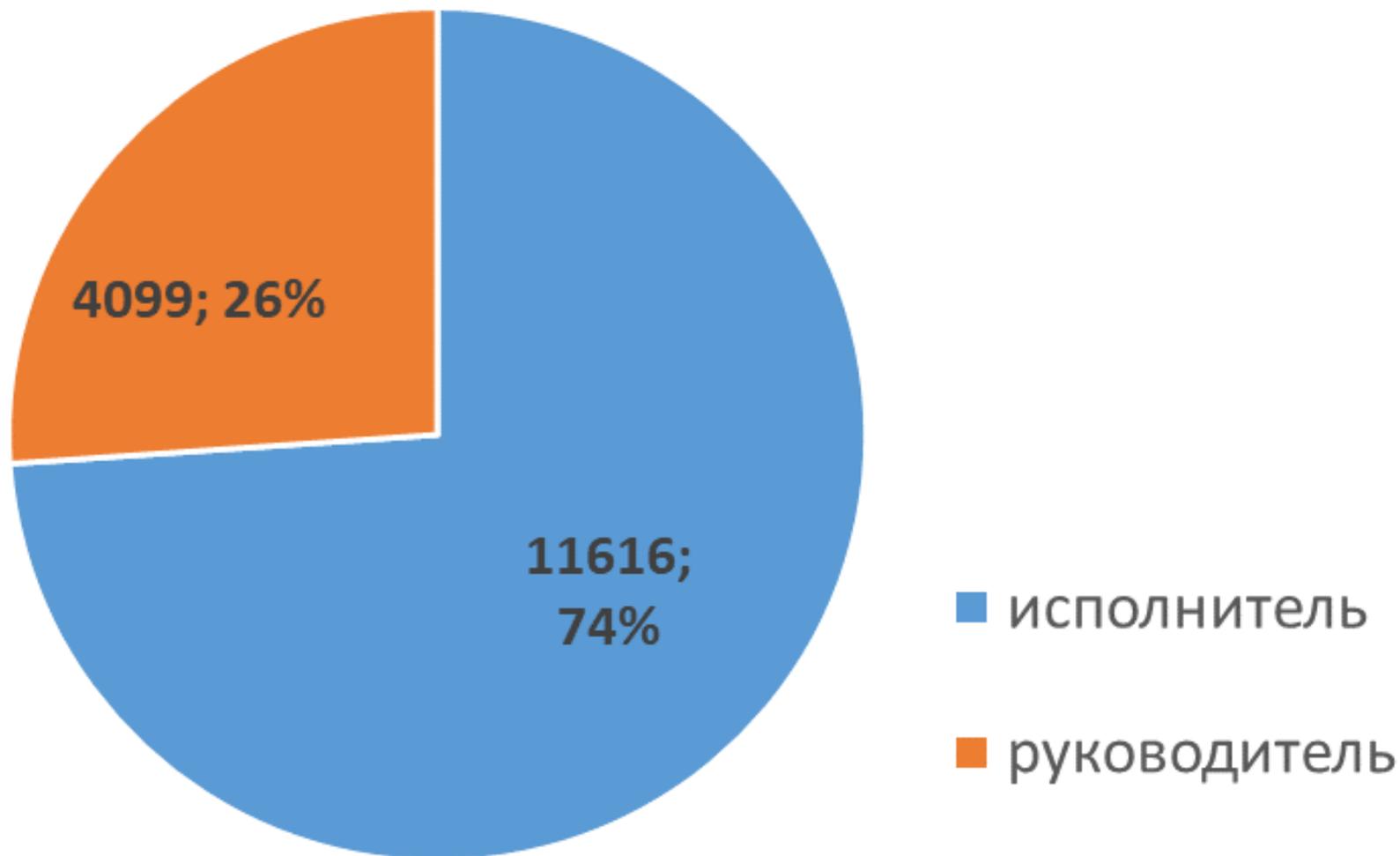
Подготовка



Email Address	Username	Submitted
[redacted]@evraz.com	[redacted]	2018-08-09 15:48:09
Valery [redacted]enko@evraz.com	fe	2018-08-09 15:52:07
Dmitry [redacted]@evraz.com	as	2018-08-09 15:56:44
Dmitry [redacted]@evraz.com	1	2018-08-09 15:57:02
Valery [redacted]enko@evraz.com	ay	2018-08-09 15:57:52
Dmitry [redacted]@evraz.com	ba	2018-08-10 14:27:44
Dmitry [redacted]@evraz.com	12	2018-08-10 14:28:04
Dmitry [redacted]@evraz.com	1	2018-08-10 15:39:16
dmitry [redacted]@evraz.com	1	2018-08-21 09:24:39

Show Passwords Refresh

Структура рассылки



Первый этап – весна 2019

Результат 20.05.2019:

Писем отправлено – 12774

Сообщили о фишинге – 103

Передали свои данные - 417

Ср 06.03.2019 11:45
"Блок по работе с финансовыми партнерами" - ██████████@evraz.com>
Сбербанк для сотрудников. Выгодные условия

Кому ██████████@evraz.com

Это сообщение было отправлено с важностью: Низкая.
При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.
Чтобы скачать рисунок, щелкните эту ссылку. Автоматическое скачивание некоторых рисунков в Outlook было отменено в целях защиты конфиденциальности.



Уважаемые коллеги!

Рады сообщить, что "ЕвразХолдинг" и ПАО "Сбербанк" запускает совместную корпоративную программу: для наших сотрудников снижены ставки по кредитам, увеличены ставки по вкладам.

Участие в программе гарантирует вам:

- Сниженные процентные ставки по потребительскому (от 10,3%) и ипотечному (от 8,5%) кредитованию;
- Увеличенный процент по вкладам (до 15,5%);
- Кредитные карты от 0%, с бесплатным обслуживанием;
- другие, особые условия сотрудничества.

Для того, чтобы принять участие, вам необходимо зарегистрироваться по ссылке ниже:

[Зарегистрироваться](#)

С Уважением,

Блок по работе с финансовыми партнерами.

Вт 19.03.2019 9:16
"Блок по работе с партнерами логистических перемещений" ██████████@evraz.com>
Проезд к местам отдыха сотрудников. Выгодные условия

Кому ██████████@evraz.com

Вы переадресовали это сообщение 19.03.2019 9:48.
Это сообщение было отправлено с важностью: Низкая.
При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.

Уважаемые коллеги!

"ЕвразХолдинг" и крупнейший транспортный оператор ПАО "РЖД" проводит совместную акцию "Летний марафон по зимним ценам" для сотрудников и родственников. Ответить правильно на 5 вопросов, получи свой уникальный код.

Участие в программе позволит Вам в летний сезон 2019 г.:

- Воспользоваться скинками до 20% - в пассажирных и до 25% - в купейных вагонах;
- Выиграть поездку в г. Анапу или г. Сочи в комфортабельном вагоне класса СВ для себя, друзей или родственников (туда и обратно, питание включено, не более 4 человек);
- Получить сувенирную продукцию (фирменные жетоны, подстаканники, ложки и др.)

Не откладывайте! Получите свою скидку прямо сейчас!

Чтобы принять участие, вам необходимо перейти по ссылке: [указовель](#), идентифицироваться на сервере - ввести данные от корпоративной учетной записи (логин, пароль). Нажать кнопку "Авторизоваться". Правильно ответить на 5 несложных вопросов. После завершения следовать дальнейшим указаниям системы.

Участие в программе совершенно бесплатно.

С Уважением,
Главное транспортно-логистическое управление.

РЖД Бонус

Для продолжения, выполните вход в систему под своей корпоративной учетной записью

Имя пользователя:

Пароль:

Второй этап – осень 2019

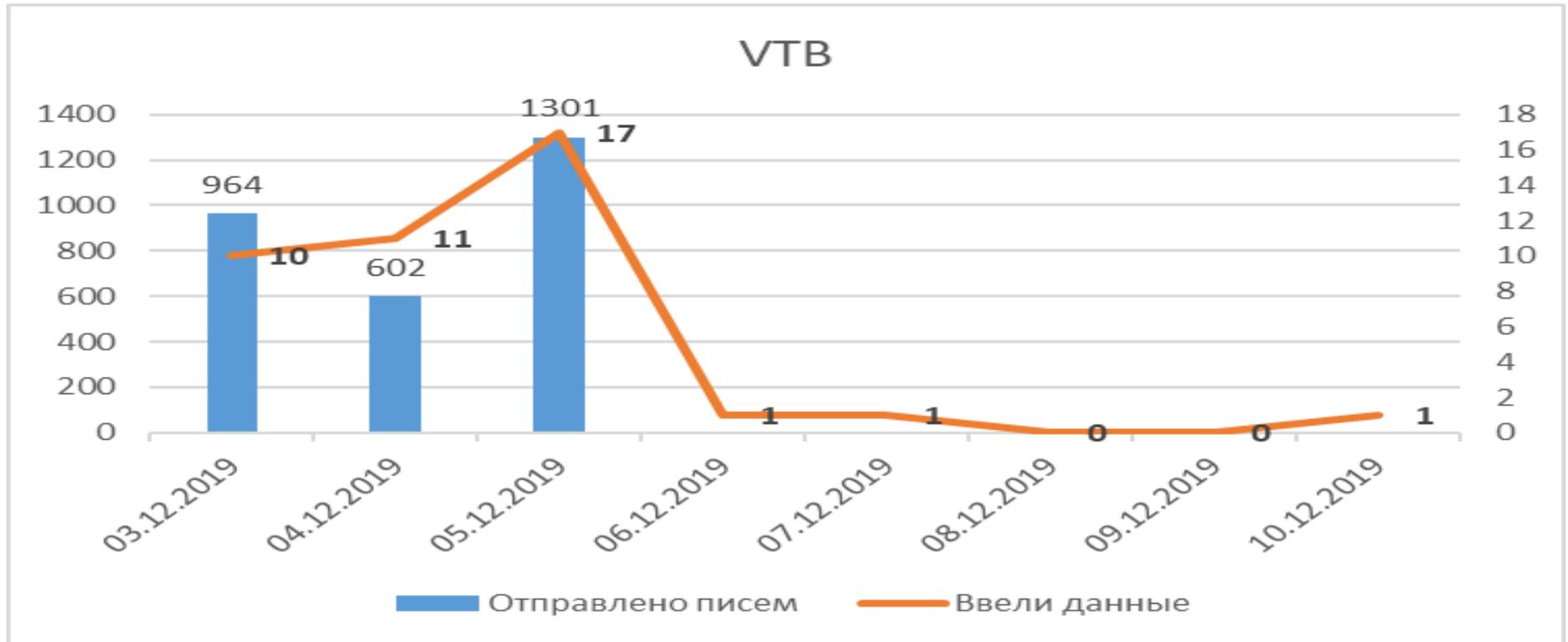
The screenshot shows the EBRAS website header with the logo and tagline "мы делаем мир сильнее". Navigation links include "7 СЭП", "События ЕВРАЗ", "ЦСР", weather information for Novokuznetsk (-7 °C), and search options for employees and the portal. A sidebar on the left lists "Объявления", "О ЕВРАЗе", "Страницы подразделений", "Последние", and "Весь контент сайта". The main content area contains a login form with fields for "Имя пользователя:" and "Пароль:", and a "Авторизоваться" button. Below the login form is a 404 error message: "Ошибка 404 ВАМ НЕ ДОСТУПЕН МУЛЬТИКАРТА ВТБ" and "нет доступа". A promotional banner for "ВТБ" offers free services, listing various banking and financial products like "мастер-счета", "счета", "кэшбэк", and "инвестиции".



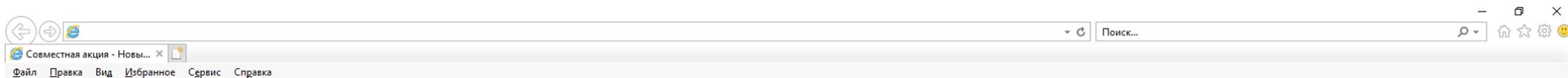
Результаты по теме «ВТБ»

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

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



Тема Пятерочка



Пятерочка г. Москва

8-800-XXX-55-05

войти

холодная

Товары по акциям | Выручай-карта | Адреса магазинов | Детский клуб | Барный клуб | Партнёры



Акции в г. Москва [Изменить город](#)

АКЦИИ В БЛИЖАЙШЕМ МАГАЗИНЕ



до 3 января
Ч.ЧУПС Карам. ЭКЗОТ-ТРОПИК с
нат.сок.12г

2+1



до 3 января
Козинак подсолнечный,
Азовская КФ, 50 г



до 3 января
ЧУПА ЧУПС Карамель ФРУТ-
ТЕЛЛА 17г



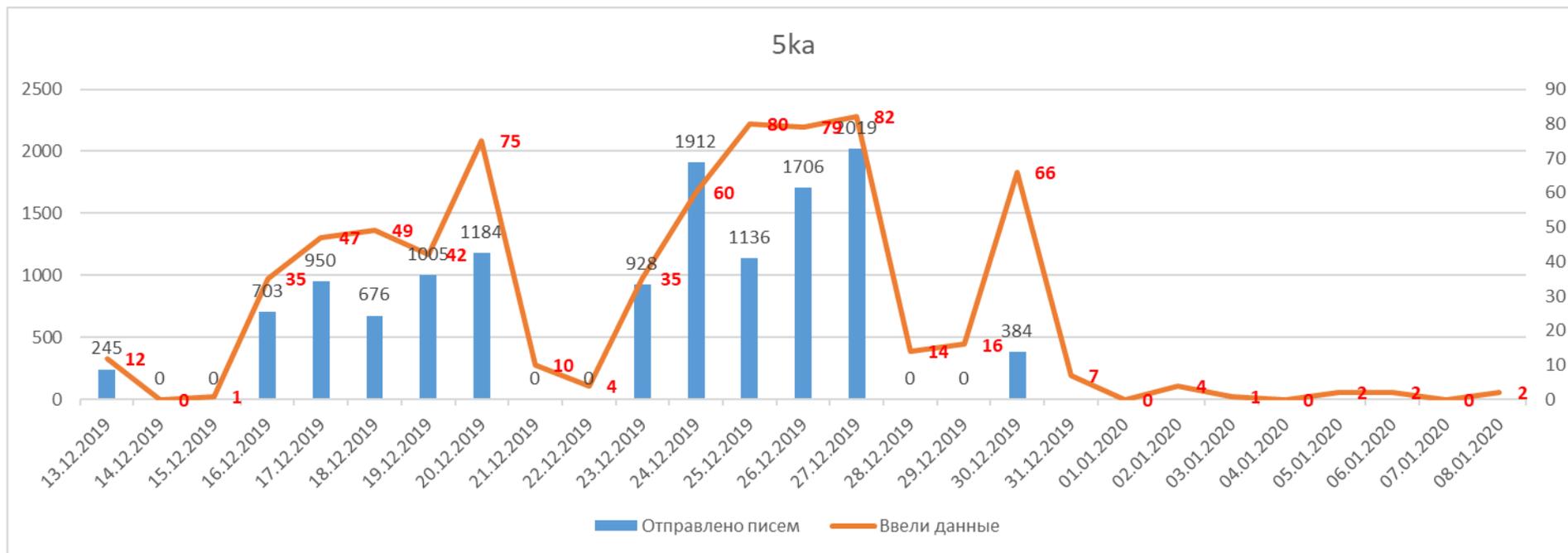
до 3 января
Батончик глазированный нуга
с мягкой карамелью
шоколадный аромат 40 г



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



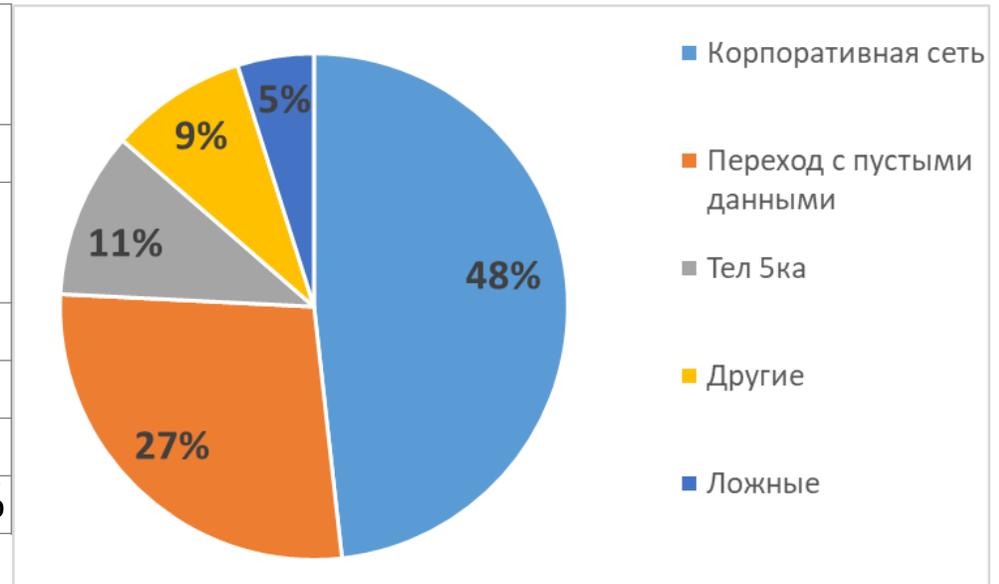
Какие данные вводили пользователи

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%



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%

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