

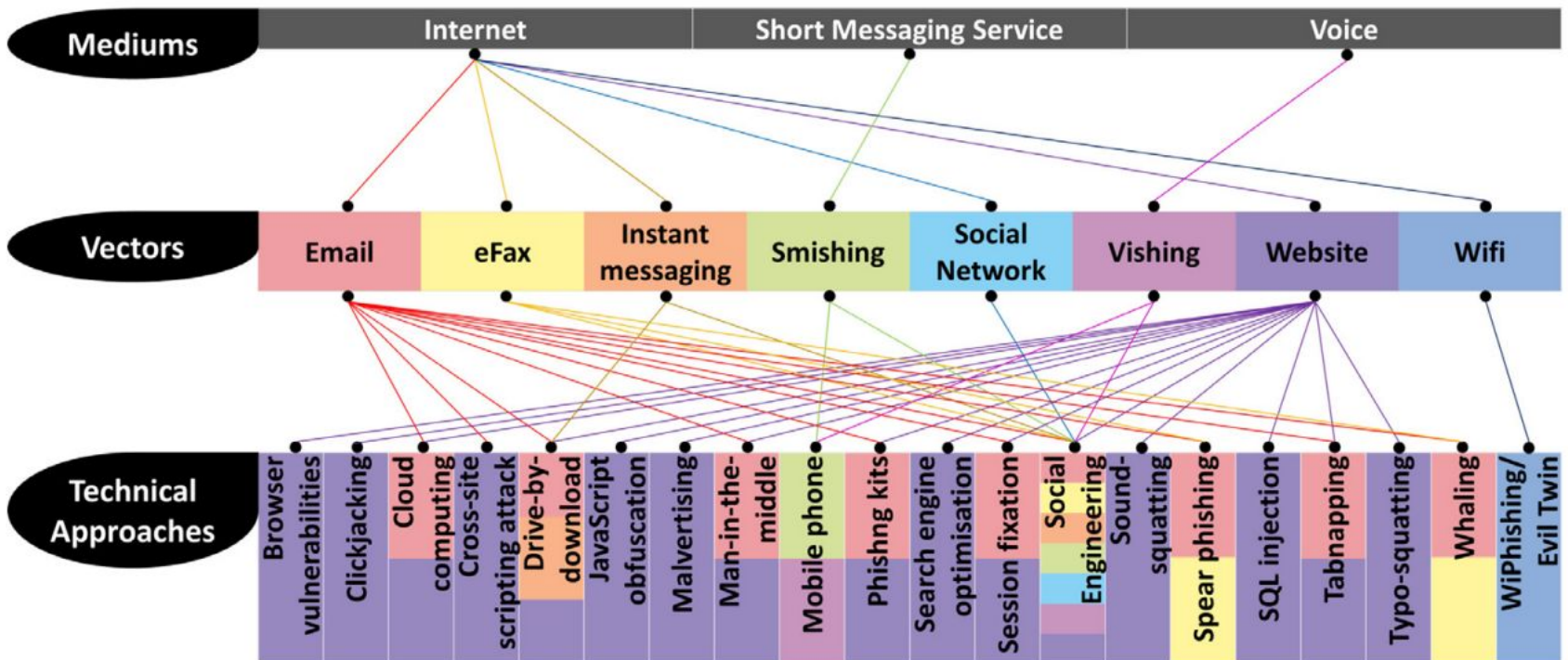
Сравнение средств и методов  
выявления и защиты от  
фишинговых атак

Коневши Р.Н.

# Что это?

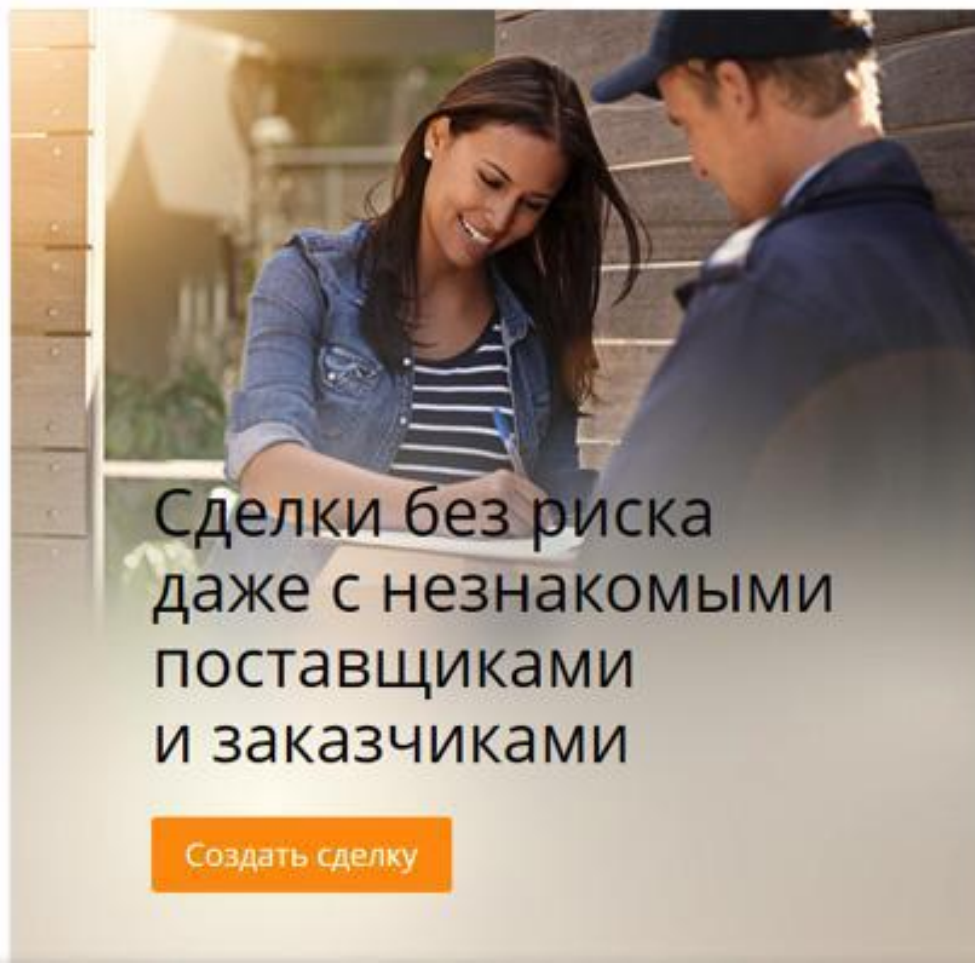
Фишинг - один из видов интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам, паролям, данным лицевых счетов и банковских карт. В основном, используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.

# Что это?



Москва > Малый бизнес > Банковское обслуживание > Сервис «Безопасная сделка»

## Сервис «Безопасная сделка»



Сделки без риска  
даже с незнакомыми  
поставщиками  
и заказчиками

Создать сделку

Надежная защита  
продавца и  
покупателя

Ваши средства будут сохранены  
на специальном счете до  
исполнения обязательств по  
договору



Быстрое  
оформление

Все сделки проводятся в режиме  
онлайн



Выгодные условия

Комиссия за сделку всего 1,45% от  
суммы договора





### Надежная защита продавца и покупателя

Ваши средства будут сохранены на специальном счете до исполнения обязательств по договору.



### Быстрое оформление

Все сделки проводятся в режиме онлайн.



### Выгодные условия

Комиссия за сделку всего 1,45% от суммы договора.



# Зона для гостей

Пожалуйста, укажите пароль:

*Пароль*

---

*Вперед*



Пожалуйста, авторизуйтесь

Номер телефона

Телефон

Код из SMS

Код

[Помочь код](#)

Войти

или

Войти через СББОП

# Зачем выявлять?

- Защитить личные данные пользователя (данные карт, ПДн, связки логин/пароль и т. д.)
- Защитить данные организации
- Не все фишинговые атаки используют вирусы

# Что рассматриваем?

- «Классический» метод
- Метод без использования средств автоматизации
- Алгоритм под кодовым названием «Phishing Destroyer»



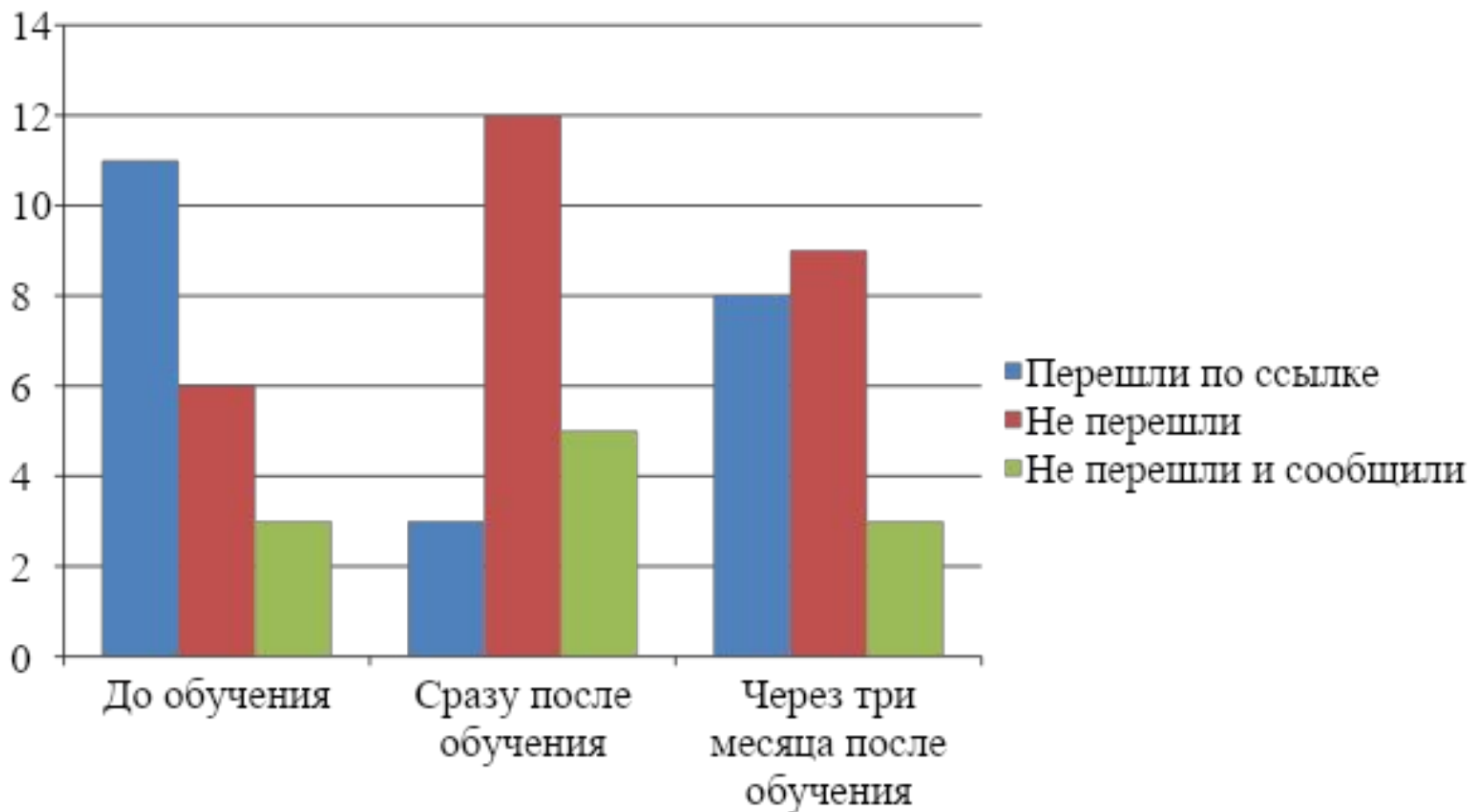
# «Классический» метод

- Проверка ссылок на вредоносность
- Проверка отправителя
- Проверка совпадения реального адреса отправителя с отображаемым

# Метод без использования средств автоматизации

- Обучение
- Информирование
- Тестирование

# Метод без использования средств автоматизации



# «Phishing Destroyer»

- Анализ текста сообщений
- Выявление общей маски фишинговых сообщений
- Использование обучения

# Как работает?

- На этапе обучения составляется матрица весов связей слов
- При повторении связи вес пересчитывается как мат ожидание имеющегося значения и нового
- На этапе анализа сообщения составляется матрица связей слов и сравнивается в с текущей матрицей
- Процент совпадения весом приводится как процент вероятности фишинга

# Проблемы

- Необходимость большой обучающей выборки
- Ошибки первого рода

Спасибо за внимание