НТЦ ВУЛКАН

Юридические предпосылки и практика контроля соблюдения прав субъектов в цифровой среде

Применение инструментов OSINT

Коваленко Д.В.

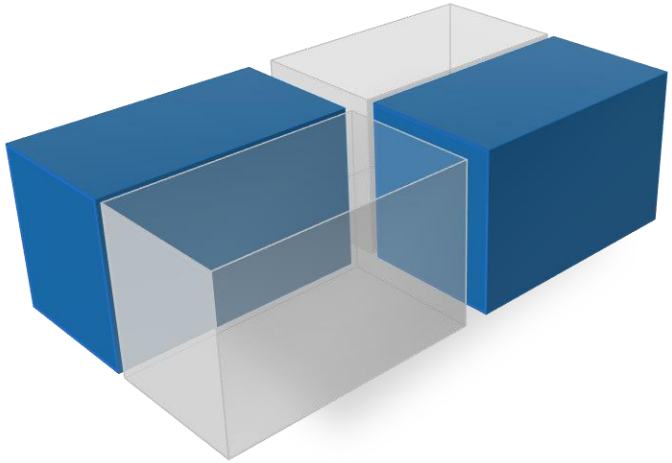
27 апреля 2021 г.

www.ntc-vulkan.ru

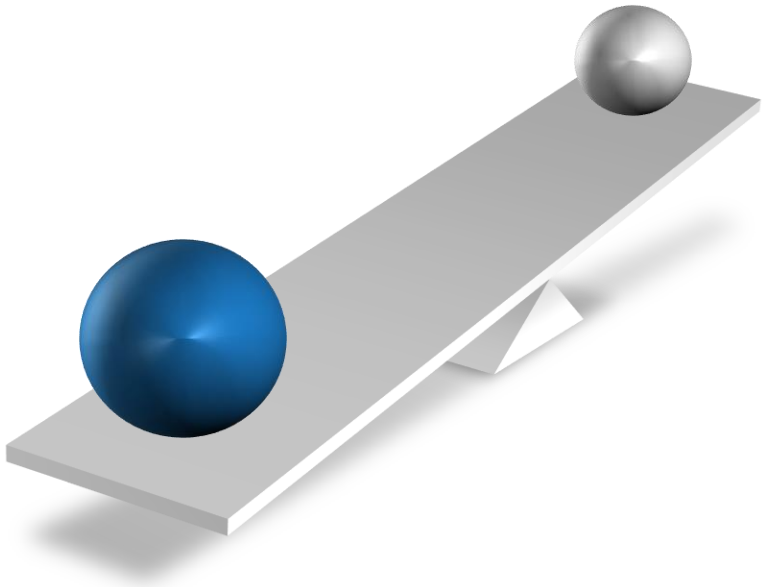
СОДЕРЖАНИЕ

- Цифровая трансформация и права субъектов
- Персональные данные в открытом доступе
- Корпоративная информация в открытом доступе
- Инструменты разведки для определения наличия данных в открытом доступе
- Способы получения персональных данных
- Сбор информации о компании
- Пример: кража исходного кода

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ И ПРАВА СУБЪЕКТОВ



Цифровая трансформация – это процесс перевода всех аспектов функционирования и взаимодействия государства, общества и бизнеса в гибридную (в т.ч. цифровую) среду



- Право на защиту персональных данных, в том числе право на забвение
- Право на защиту коммерческой тайны

ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ОТКРЫТОМ ДОСТУПЕ

Проблема: персональными данными пользуются злоумышленники в фишинг и вишинг атаках.



Право на забвение – способ сокращения персональной информации в открытом доступе.

Правовые механизмы:

- Консультирование гражданина
- Консультирование оператора ПДн
- Мониторинг по заданию регулятора

КОРПОРАТИВНАЯ ИНФОРМАЦИЯ В ОТКРЫТОМ ДОСТУПЕ

Проблемы:

1. Возможность получения списка сотрудников
2. Утечки закрытой информации о деятельности компании
3. Споры между юридическими лицами

Правовые механизмы:

- Непроцессуальное исследование
- Внесудебная компьютерная экспертиза
- Судебная компьютерная экспертиза

ВЫЯВЛЕНИЕ НАЛИЧИЯ ДАННЫХ В ОТКРЫТОМ ДОСТУПЕ

OSINT – это разведка на основе открытых источников

Инструменты и технологии OSINT позволяют получить:

- ФИО
- Номер телефона
- Электронный адрес
- Физический адрес
- Никнейм
- Идентификаторы личности
- Информация об интересах человека
- Корпоративные ресурсы
- Исходный код
- Информация о деятельности компании



СПОСОБЫ ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 Расширенные возможности поисковых систем

Google Dorking. В частности, поиск и анализ документов, фотографий

2 Анализ социальных сетей

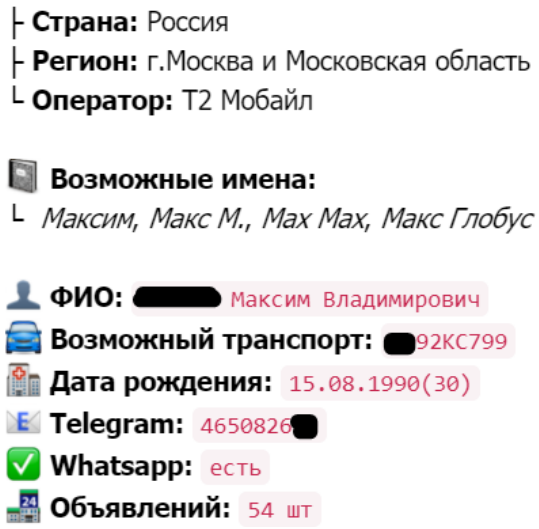
Извлечение персональных данных, выявление круга общения, определение интересов

3 Поиск по базам утечек

Телеграм бот eye of god, Lampyre

4 Узкоспециализированные инструменты

Nuga.app, namecheck и др.



СБОР ИНФОРМАЦИИ В ОТКРЫТОМ ДОСТУПЕ

1 Анализ документов компании

FOCA для извлечения мета-данных

2 Поиск общедоступной информации о финансовых и имущественных отношениях

Aleph data, отчеты компании, СМИ

#	Domain	Email	Email Source
1	cisco.com	ciscowebexstart1@cisco.com	RedditPost Search for Emails
2	cisco.com	dewittic@cisco.com	Exalead DOCX Search for Emails
3	cisco.com	bclaise@cisco.com	Exalead DOCX Search for Emails
4	cisco.com	mickpayn@cisco.com	Exalead DOCX Search for Emails
5	cisco.com	jshake@cisco.com	Exalead DOCX Search for Emails
6	cisco.com	wfoxr@cisco.com	Exalead XLSX Search for Emails
7	cisco.com	jdayu@cisco.com	Exalead XLSX Search for Emails
8	cisco.com	acampbell15@cisco.com	Exalead XLSX Search for Emails
9	cisco.com	RISPEYER@CISCO.COM	Exalead XLSX Search for Emails
10	cisco.com	gosland@cisco.com	Exalead XLSX Search for Emails
11	cisco.com	hbarrass@cisco.com	Exalead XLSX Search for Emails
12	cisco.com	lindsayd@cisco.com	Exalead Search for Emails
13	cisco.com	DScruggs@cisco.com	Exalead Search for Emails

3 Анализ и подбор данных сотрудников

Инструменты автоматизации поиска: Spiderfoot, Recon-ng, OSRFramework. Simplyemail для подбора email адресов

4 Анализ сайта компании

Поиск скрытых материалов, корпоративных ресурсов, старых версий

ПРИМЕР: КРАЖА ИСХОДНОГО КОДА

Способы получения исходного кода страницы из открытых источников:

- Репозитории с кодом
- Утечки на стороне компании разработчика ПО
- Резервные копии или системы контроля версий
- Комментарии

Далее для подтверждения факта кражи можно провести экспертизу персональных компьютеров сотрудников компании

НТЦ «Вулкан» - независимый эксперт и интегратор технологий информационной безопасности



На рынке с **2010** года

Комплексные решения в сфере экономической и информационный безопасности

500+ реализованных проектов в ИБ

20+ проектов внедрения SIEM

150+ сотрудников в штате

Сертифицированная система менеджмента качества

Входит в **30** крупнейших компаний РФ в сфере защиты информации

По версии CNews Analytics, 2019

Допуски и лицензии ФСТЭК, ФСБ, Минобороны, Минпромторг

Партнер IBM по группе продуктов Security с 2010 года

IBM Platinum Business Partner

Развитие партнерских отношений с международными и российскими вендорами и производителями в сфере ИБ

НТЦ ВУЛКАН

Юридические предпосылки и практика контроля соблюдения прав субъектов в цифровой среде

СПАСИБО ЗА ВНИМАНИЕ!

НТЦ ВУЛКАН

www.ntc-vulkan.ru