Александр Вураско
ведущий аналитик ГК «Инфосекьюрити»

vurasko@in4security.com
Тел. +7 903 787 17 89

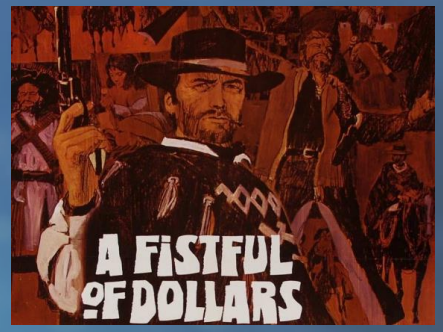
1. Информационная безопасность никогда не находится в статике

2. Современные угрозы требуют современных методов противодействия

3. Перечень угроз куда шире, чем кажется

4. Процессы, проистекающие внутри компании, находят отражение за ее пределами

Популярность высоких технологий у современных преступников



Концепция: «киберпреступление как услуга»:
- низкий порог вхождения
- доступный инструментарий для совершения преступлений
- не нужно обладать глубокими познаниями в IT-сфере

Широкий круг охвата потенциальных жертв

Простота вывода денежных средств

Транснациональный характер сети

Возможности анонимизации

СТАТИСТИКА

~50%

веб-приложений
содержат уязвимости

~129 дней

уходит на исправление
критической уязвимости

56%

доля систем с тривиальной
сложностью преодоления
сетевого периметра

36%

доля успешных атак
с получением доступа
к конфиденциальным данным

** по данным Application Security Statistics Report 2017 и Positive Technologies за 2016-2018 гг.*

ЦЕЛИ И РЕЗУЛЬТАТЫ

Обнаружение уязвимостей и подготовка рекомендаций по их устранению

Определение направлений дальнейшего совершенствования системы ИБ

Устранение уязвимостей в инфраструктуре компании

Выполнение требований контролирующих органов и соблюдение стандартов

Обоснование бюджета на повышение уровня ИБ

СТАНДАРТЫ И МЕТОДОЛОГИИ

Приказы ФСТЭК России № 17, 21, 31

Международная программа
Certified Ethical Hacker

Standards for Information Systems Auditing
(ISACA)

OSSTMM v3.0 (Open Source Security Testing
Methodology Manual)

OWASP Testing Guide v4

СЦЕНАРИИ ТЕСТИРОВАНИЯ

BLACK BOX

Пентестер воспроизводит действия внешнего злоумышленника, имеющего общее представление об атакуемых объектах из открытых источников.

GREY BOX

Пентестер имитирует действия хакера, обладающего знаниями об атакуемом объекте. Уровень и глубина знаний определяется заказчиком.

WHITE BOX

Пентестер обладает всеми правами доступа администратора, и имеет полное представление об инфраструктуре организации.

ВИДЫ ПЕНТЕСТОВ

Внешний пентест и тестирование веб-приложений (Black, Grey box)

Внутренний пентест информационных систем (Black, Grey box)

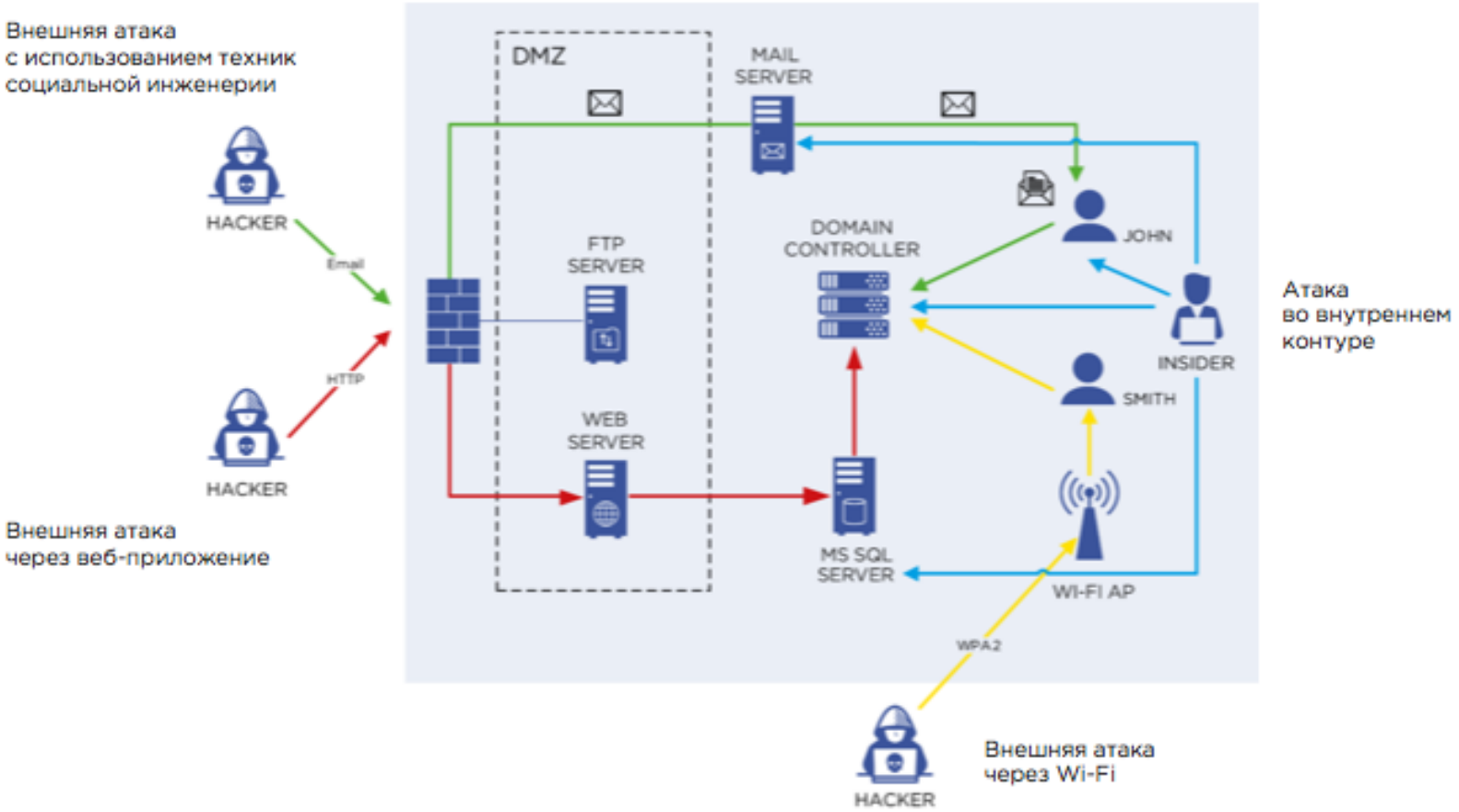
Пентест точек доступа Wi-Fi (Black box)

Социотехнический пентест (Black, Grey box)

Внутренний аудит безопасности (White box)

Структура современного преступного сообщества

СХЕМА ВОЗМОЖНЫХ АТАК, ПРОИЗВОДИМЫХ ПРИ ПЕНТЕСТАХ



ВНЕШНИЙ ПЕНТЕСТ
И ТЕСТИРОВАНИЕ ВЕБ-ПРИЛОЖЕНИЙ

- Поиск в интернете сайтов заказчика и поддоменов
- Сканирование портов и определение служб, использующих их
- Идентификация используемого ПО и технологий
- Поиск и анализ уязвимостей приложения, входящих в классификацию OWASP
- Проведение атак, направленных на эксплуатацию уязвимостей (по согласованию с заказчиком)
- Анализ результатов и подготовка рекомендаций

ВНУТРЕННИЙ ПЕНТЕСТ ИНФОРМАЦИОННЫХ СИСТЕМ

- Подключение к пользовательскому сегменту сети
- Анализ трафика протоколов канального и сетевого уровней
- Инструментальное сканирование ресурсов внутренней сети
- Поиск уязвимостей на обнаруженных ресурсах
- Проведение сетевых атак и атак, эксплуатирующих уязвимости
- Получение локальных и доменных учетных записей
- Анализ результатов и подготовка рекомендаций

ПЕНТЕСТ ТОЧЕК ДОСТУПА WI-FI

- Изучение характеристики и особенностей сетей Wi-Fi на объекте
- Проведение атак на аутентификацию и авторизацию в беспроводных сетях
- Получение ключей шифрования между клиентом и точкой доступа Wi-Fi
- Проведение атак на аппаратное обеспечение сетей Wi-Fi
- Установка поддельной точки доступа Wi-Fi, проведение атак на клиентов сетей
- Обработка результатов и подготовка рекомендаций

СОЦИОТЕХНИЧЕСКИЙ ПЕНТЕСТ

- Сбор данных об объекте и пользователях
- Подготовка провоцирующих данных
- Рассылка по электронной почте, целевое общение через соцсети и мессенджеры
- Личные звонки (телефон, Skype)
- Распространение носителей информации с провоцирующими данными
- Оценка преодоления физического периметра (скрытное копирование ключей СКУД)
- Анализ результатов и проведение обучения

ВНУТРЕННИЙ АУДИТ БЕЗОПАСНОСТИ

- Автоматизированная инвентаризация IT-активов
- Проверка актуальности версий ПО, ошибок конфигурации серверов и сетевого оборудования
- Поиск и анализ уязвимостей средств защиты
- Проверка соответствия стандартам ИБ (PCI DSS, NIST, NERC и др.)
- Анализ возможности проведения сетевых атак (Spoofing, MiTM)
- Построение векторов атак и подготовка плана для минимизации рисков ИБ


INFOSECURITY
AWARENESS:
ОБУЧЕНИЕ
ПО ВОПРОСАМ ИБ

Все совершают ошибки

От невнимательности

От незнания

Социальная инженерия

Социальная инженерия

СТАТИСТИКА

Согласно данным статистики, 2/3 инцидентов ИБ являются результатом действий сотрудников компании.

40% компаний

не имеют стратегии информационной безопасности

56% компаний

не имеют разработанного процесса реагирования на инциденты

48% компаний

не имеют программы обучения нормам и требованиям ИБ

* данные PWC по итогам опроса 248 российских компаний в 2017 году

КОМПЛЕКСНЫЙ ПОДХОД

Мы анализируем текущее состояние осведомленности об угрозах ИБ,
а затем организуем комплексное обучение сотрудников компании.

ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ ПО ВОПРОСАМ ИБ

Очное обучение

Дистанционное обучение

Контроль эффективности

Дополнительные материалы

Отчетность по сервису

ОЧНОЕ ОБУЧЕНИЕ

Теоретическая информация усваивается лучше, когда ее подача сопровождается живым общением.

Тренинги

Семинары

Вы можете выбрать тему из нашей базы или предложить собственную

Занятия проводятся в том числе с применением кейс-метода

По итогам занятия обучающимся предлагается пройти тестирование

ДИСТАНЦИОННОЕ ОБУЧЕНИЕ

Сотрудники могут пройти полное обучение в удобное для них время, не покидая рабочего места.

Электронные курсы

Видеоролики GoAnimate

Рассылки Security Tips

Вебинары

Обучение проводится по модульному принципу (гибкая комплектация материалов)

Мы уделяем основное внимание практическим вопросам, конкретным кейсам и проблемам

Наши учебные материалы можно просматривать на разных типах электронных устройств

ЭЛЕКТРОННЫЕ КУРСЫ

Для разработки курсов мы используем профессиональный комплекс программ Articulate 360. Готовые курсы упаковываются в стандартный SCORM-пакет.

ПЕРСОНАЛИЗАЦИЯ **ГЕЙМИФИКАЦИЯ** **МИКРООБУЧЕНИЕ**

Возможно создание обучающих курсов в Microsoft PowerPoint.

КОНТРОЛЬ ЭФФЕКТИВНОСТИ

Эффективность обучения анализируется и отражается
в конкретных количественных показателях.

**Тестирования,
упражнения и кейсы**

Образовательные игры

**Учебные фишинговые
рассылки**

Пользователи закрепляют полученные знания
в классической или альтернативной форме

Все проверочные материалы готовятся
с учетом сферы вашей деятельности

По результатам контроля эффективности
предоставляется детальная отчетность

ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ

Текстовые и графические материалы делают обучение более разнообразным и запоминающимся.

Памятки и брошюры

Карточки и лонгриды

Плакаты

Скринсейверы

Стикеры

К разработке контента привлекаются профессиональные дизайнеры и иллюстраторы

Мы готовим уникальные текстовые материалы или предоставляем качественный рерайт

Вы сами устанавливаете периодичность размещения обучающего контента

ИНДИВИДУАЛЬНАЯ ПРОГРАММА ОБУЧЕНИЯ

Пакет материалов составляется с учетом конкретных задач обучения и целевой аудитории (возраст, должность, опыт работы и т.п.).

Обучение новых сотрудников

Начальные знания

Базовые навыки

Обучение действующих сотрудников

Новые методики, стандарты, формы, программы, системы

Изменения в бизнес-процессах компании

Повышение квалификации

Конкретные темы, направления, области, компетенции

ЭТАПЫ

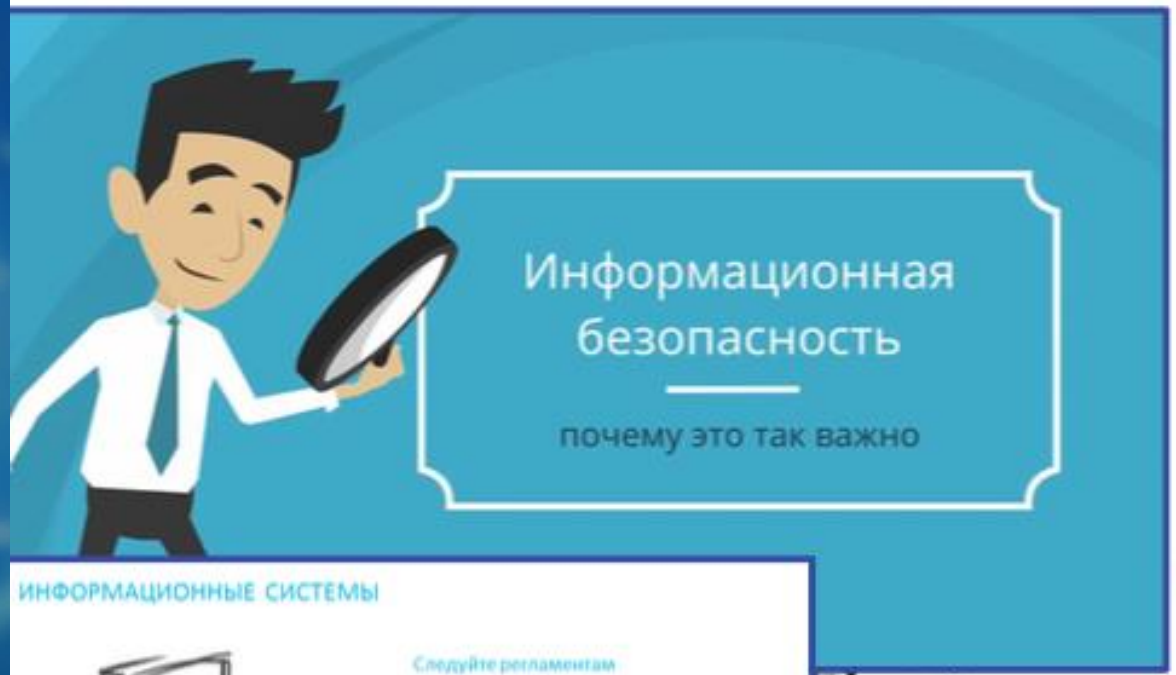
1 ОПРЕДЕЛЯЕМ ЦЕЛЕВУЮ АУДИТОРИЮ

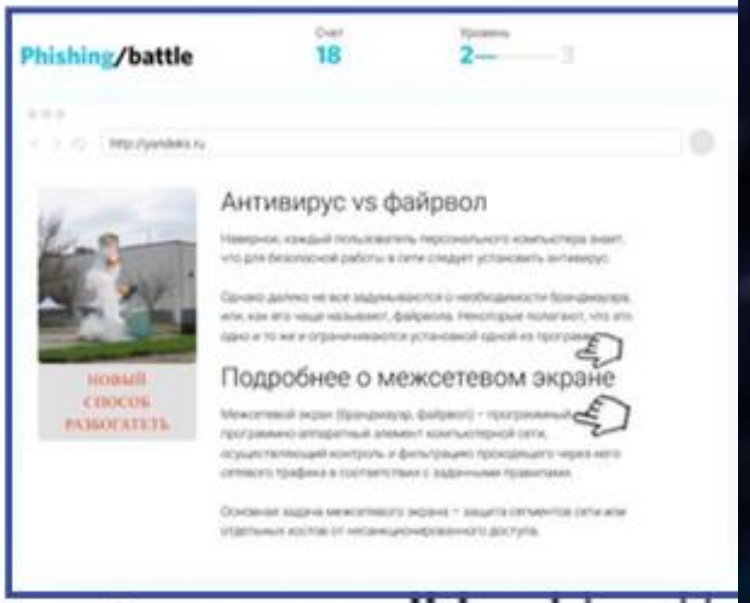
2 ГОТОВИМ И СОГЛАСУЕМ ОБУЧАЮЩИЙ КОНТЕНТ

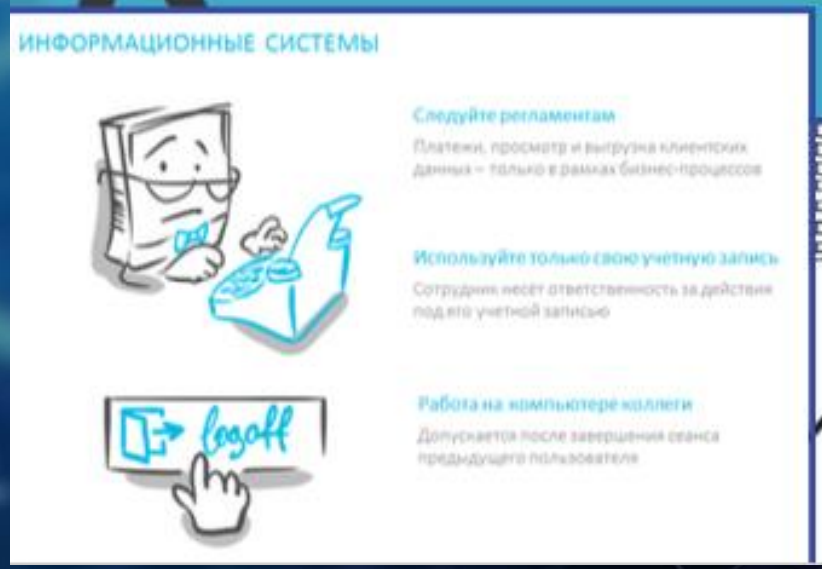
3 ПРОВОДИМ ОБУЧЕНИЕ

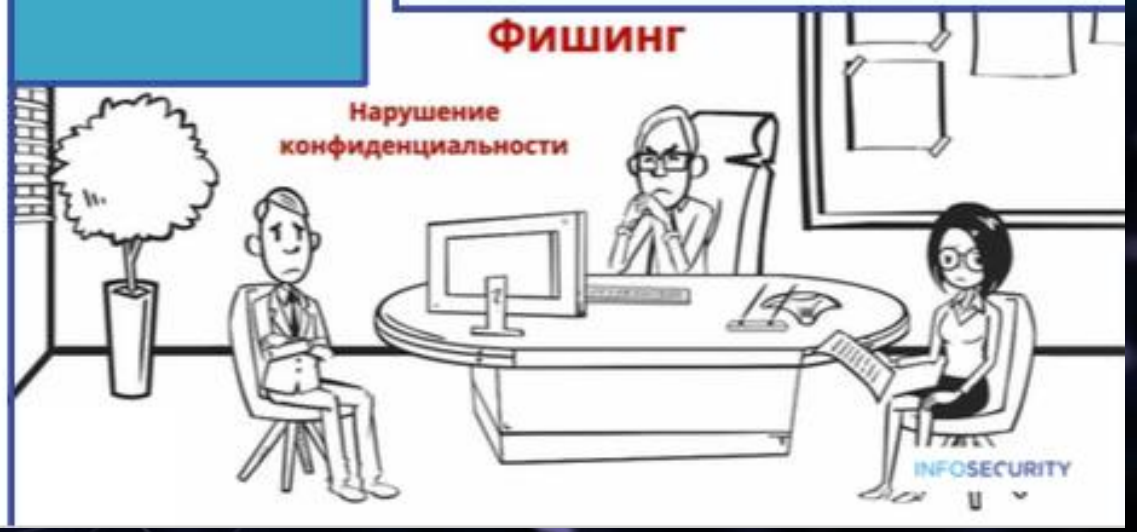
4 ПОЛУЧАЕМ ОБРАТНУЮ СВЯЗЬ И ДОРАБАТЫВАЕМ КОНТЕНТ

ПРИМЕРЫ ОБУЧАЮЩИХ МАТЕРИАЛОВ









ПРИМЕРЫ ОБУЧАЮЩИХ МАТЕРИАЛОВ

В этом выпуске Security Tips мы расскажем о правилах безопасного обсуждения рабочих вопросов и о том, почему эти правила важно соблюдать.

ЗАЩИЩАЙТЕ ИНФОРМАЦИЮ

Задумываетесь ли вы о безопасности конфиденциальной информации, когда обсуждаете с коллегами рабочие моменты в опен спейсе, лифте, кафе или на парковке? Бронируете ли переговорную комнату, если предстоит важный деловой разговор? Представляете ли, что может стать результатом случайно подслушанной фразы?

Последствия разглашения конфиденциальной информации могут быть действительно серьезными. Для компании это потеря конкурентных преимуществ и клиентов, санкции со стороны регулирующих органов, утрата деловой репутации. Для сотрудника, допустившего разглашение, — ухудшение атмосферы в коллективе, денежный штраф, выговор или даже увольнение. Чтобы избежать этих неприятностей, достаточно следовать рекомендациям Службы ИБ.

ВЕДИТЕ ПЕРЕГОВОРЫ ПРАВИЛЬНО

Не устраивайте совещаний в кафе или столовой

Если вы вынуждены обсуждать рабочие процессы во время обеденного перерыва, постарайтесь, чтобы сидящие рядом люди не стали невольными слушателями ваших переговоров. Старайтесь говорить тише, особенно если этого требует характер обсуждаемой информации. Следите за тем, чтобы не допустить разглашения персональных данных своих коллег — например, размера их заработной платы.

01 Что такое фишинг?

02 Как это работает?

03 Кто становится жертвой фишинга?

04 Я слышал про вирусы WannaCry и Petya. Они как-то связаны с фишингом?

05 Как распознать фишинговое письмо?

01

Что такое фишинг?

Слово «фишинг» (phishing) появилось в результате соединения двух английских слов — fishing (рыбная ловля, выуживание) и password (пароль). Так называют один из видов интернет-мошенничества. Цель фишинга — получить доступ к конфиденциальным данным пользователя. Злоумышленники могут украсть у вас не только логин и пароль от сайта или электронной почты, но и номер телефона, данные банковской карты. А еще сделают это тех, что вы передадите им эту информацию сами.

БАЗОВЫЙ НАБОР ТЕМ ОБУЧЕНИЯ

Конфиденциальная информация и правила работы с ней

Место ИБ в бизнес-процессах компании

Информационная безопасность на рабочем месте

Информационная безопасность при удаленной работе

Уменьшение рисков информационной безопасности

Персональные данные: понятие, обработка, защита

Программно-технические средства обеспечения ИБ

Криптография: базовые знания о науке шифрования

Социальная инженерия: способы борьбы с мошенниками

Законодательная и нормативно-правовая база ИБ

НАШИ ПРЕИМУЩЕСТВА

Мы гарантируем действительно эффективное обучение по вопросам информационной безопасности.

Повышаем осведомленность в сфере ИБ в различных формах по выбранным каналам

СИСТЕМНОСТЬ

Разрабатываем обучающий контент с учетом вашего фирменного стиля (согласно брендбуку)

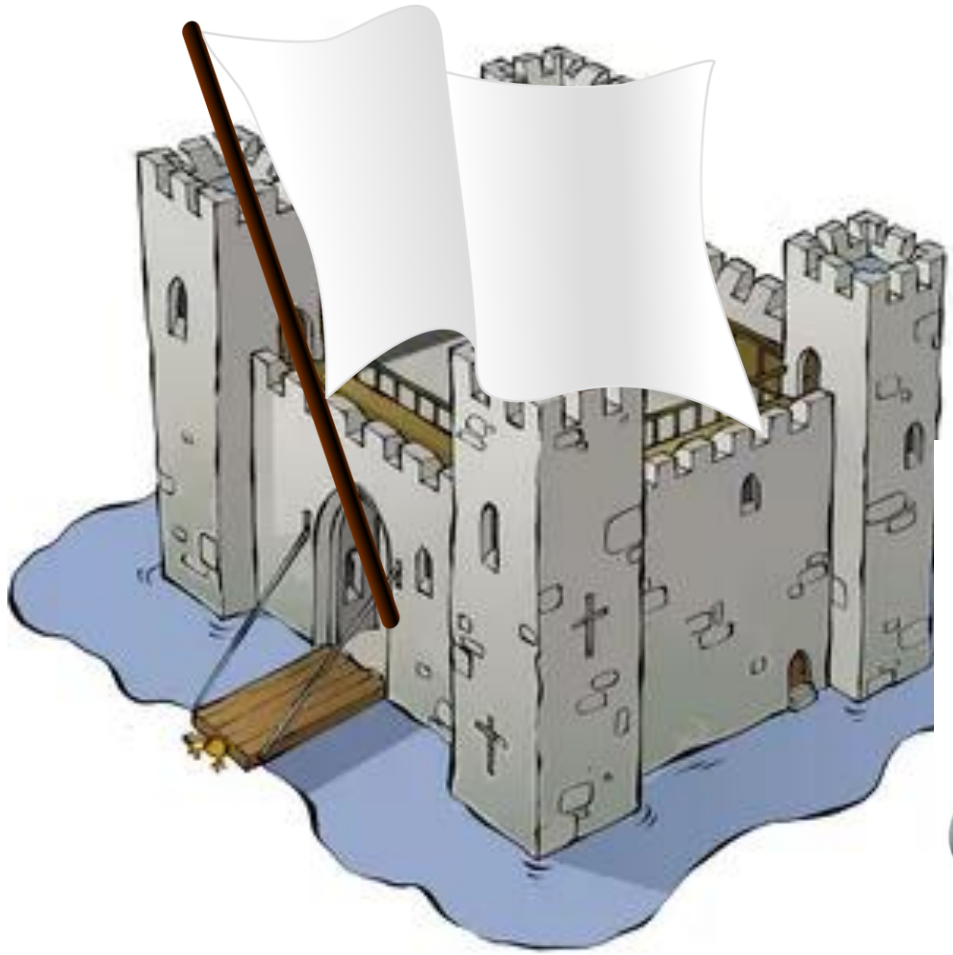
КРЕАТИВНОСТЬ

Излагаем учебный материал простым и понятным языком независимо от выбранной темы

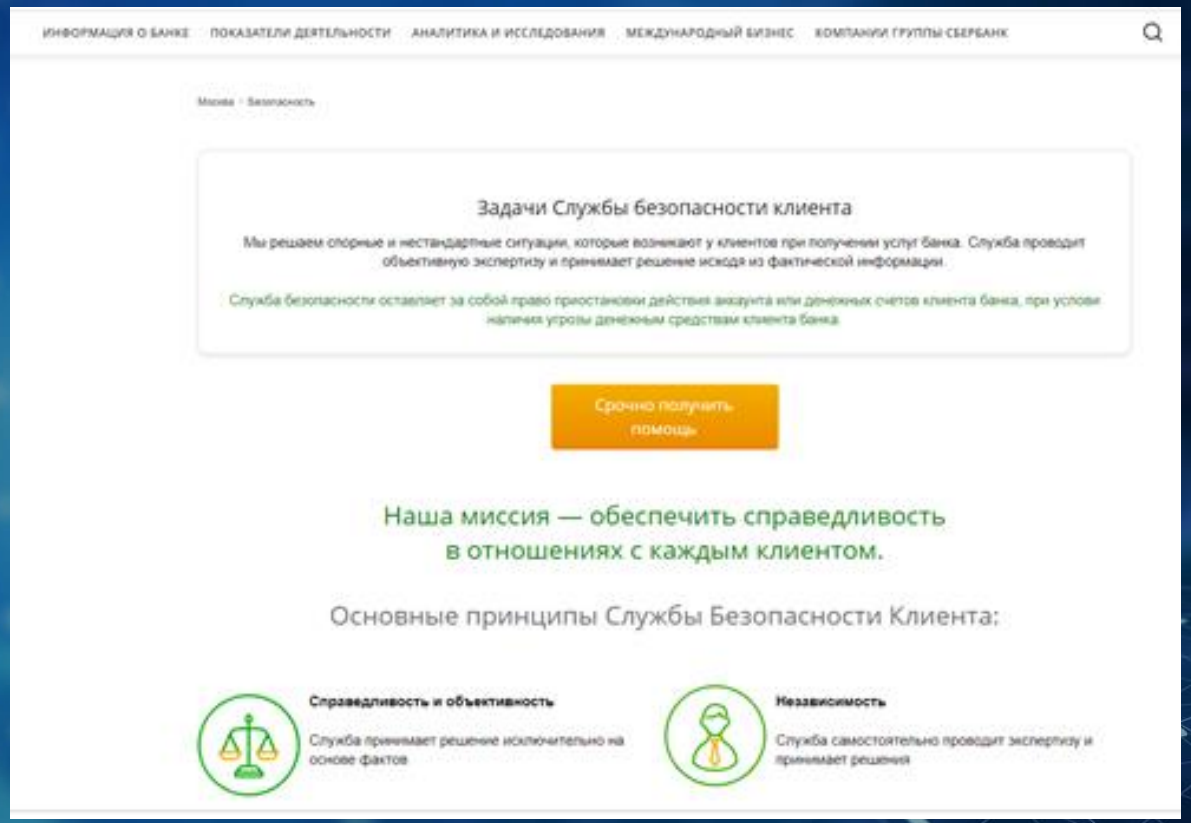
ДОСТУПНОСТЬ

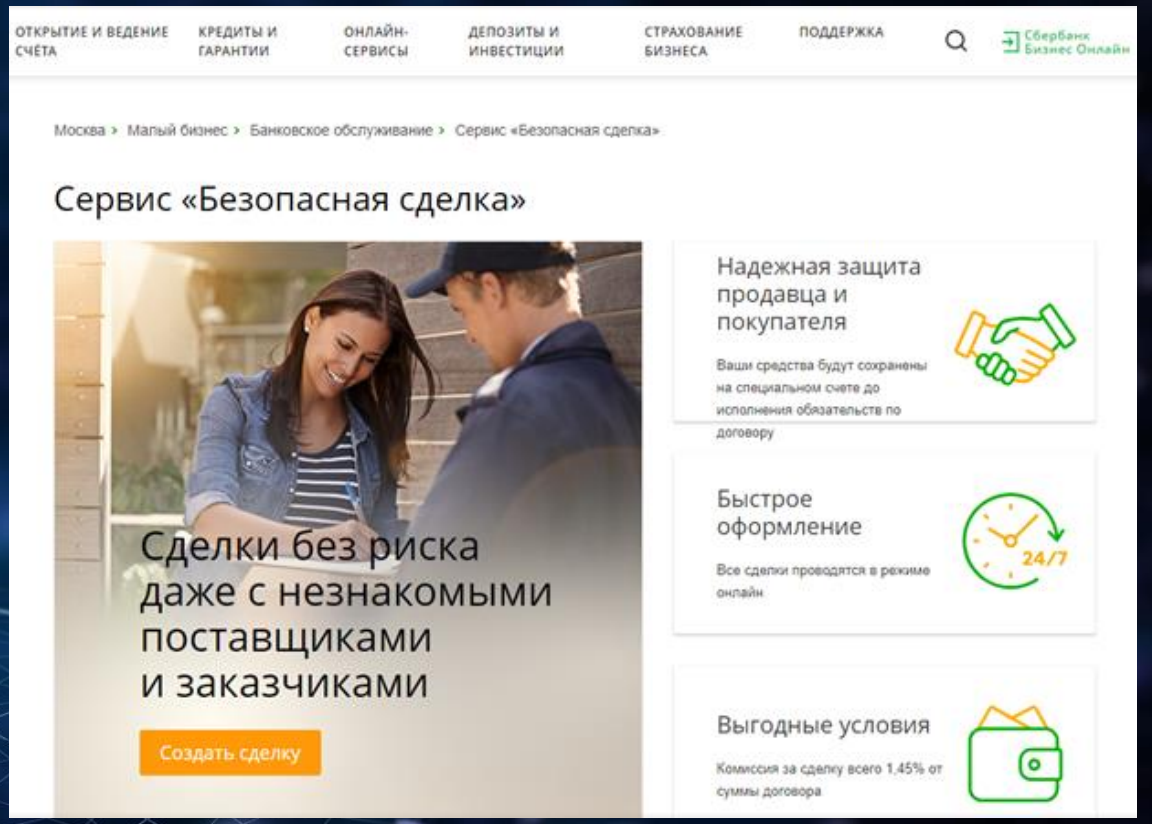
Традиционная концепция обеспечения ИБ

и ее минусы…



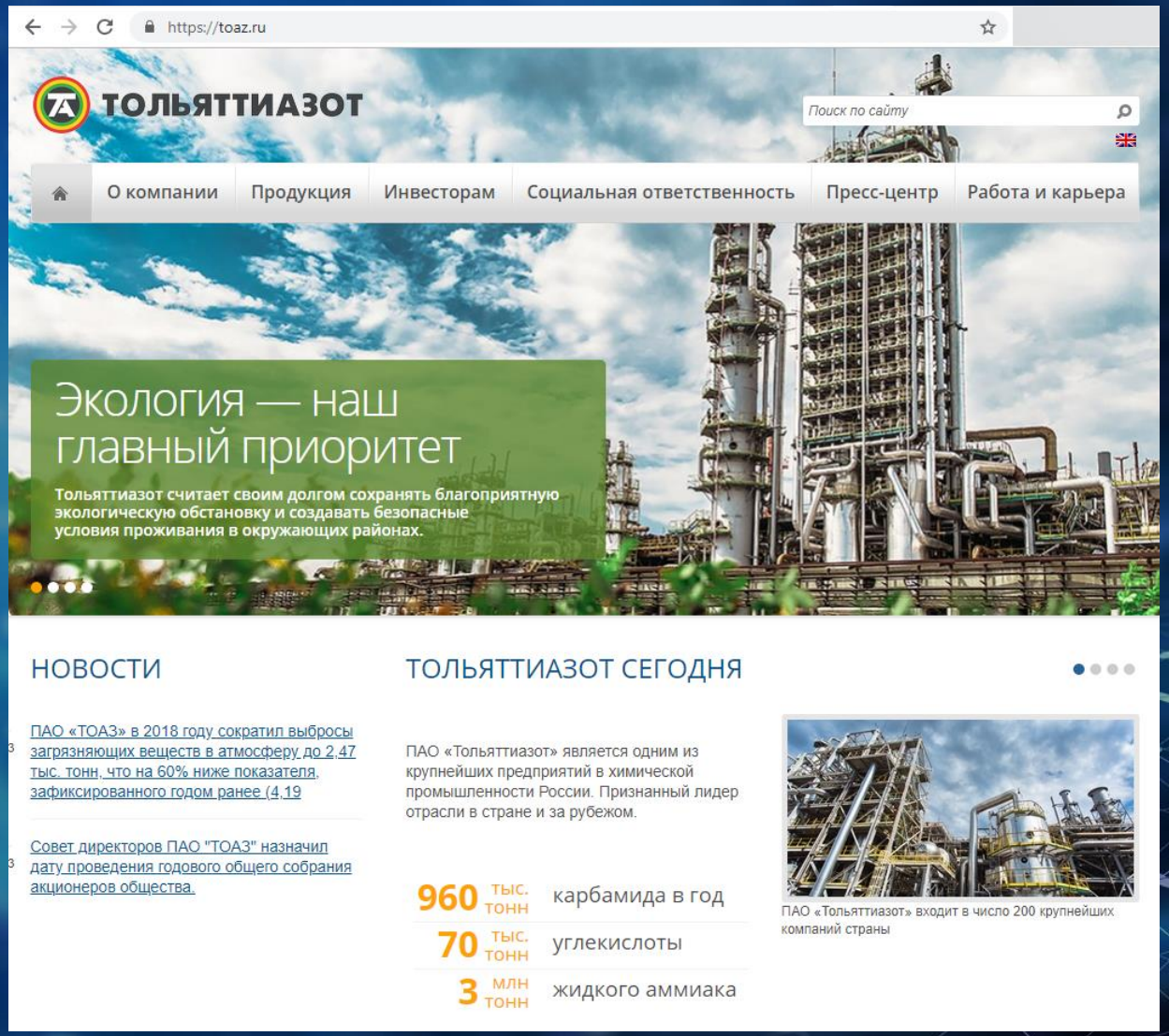
ФИШИНГ

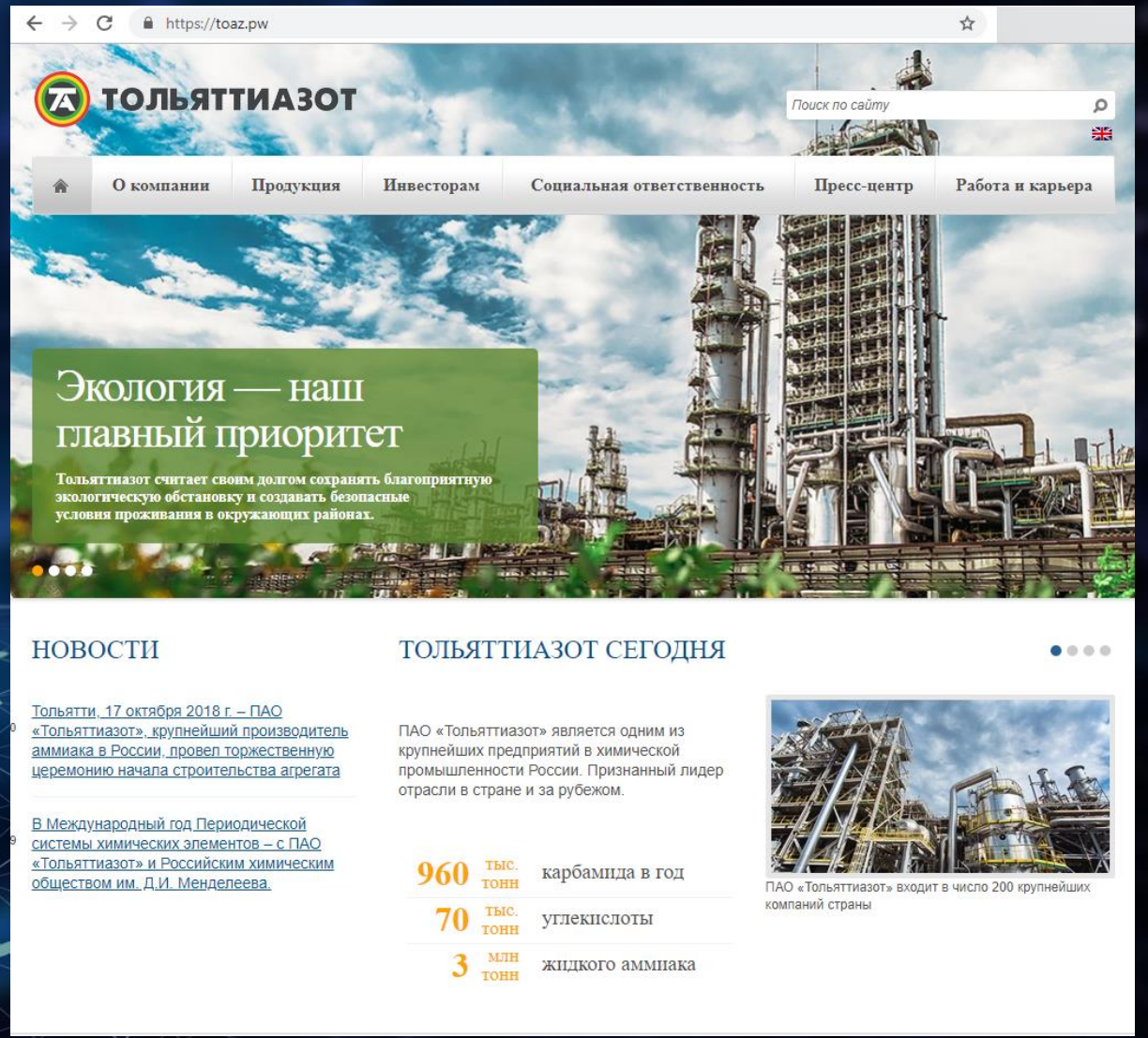


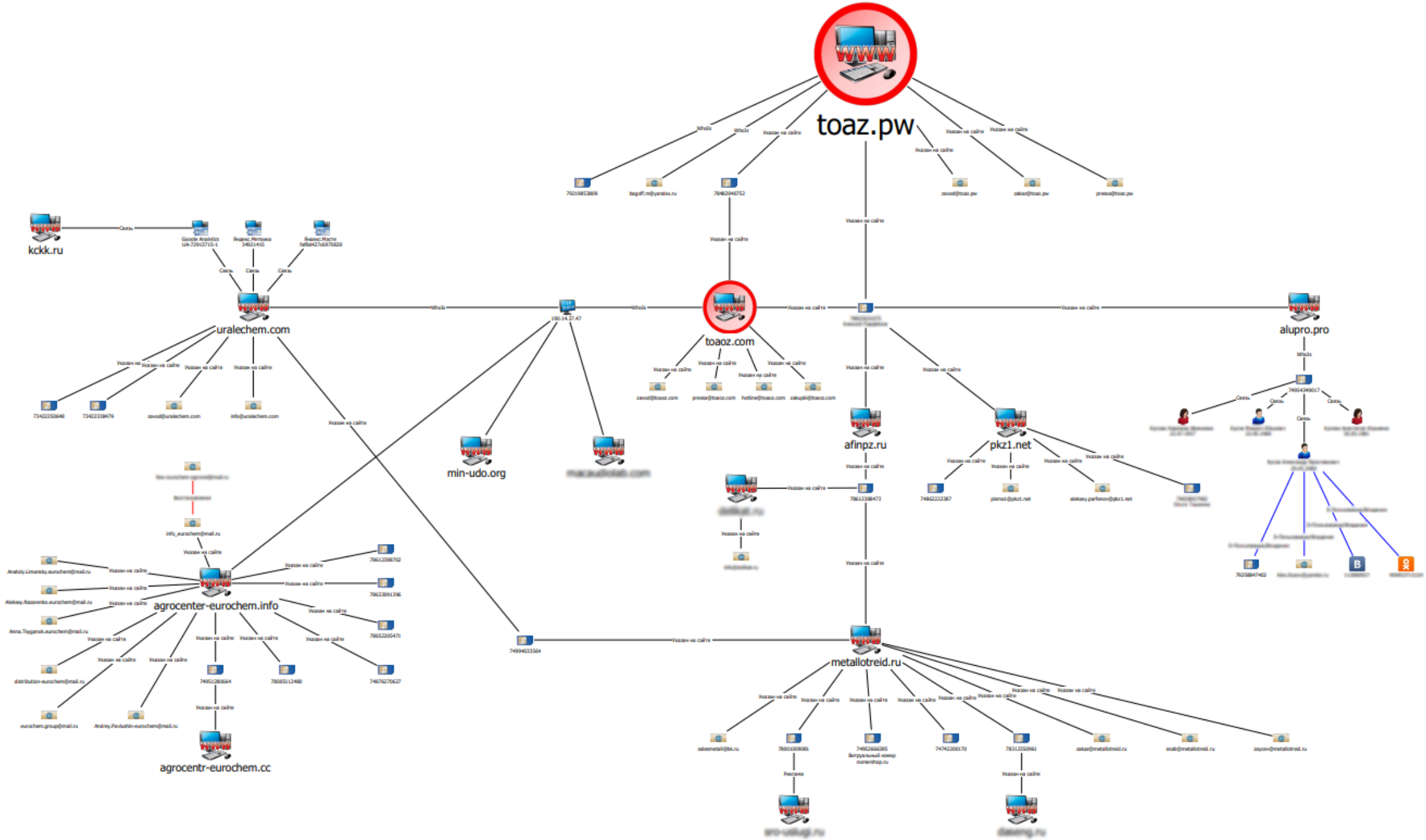


Спустя всего 7 дней после запуска сервиса

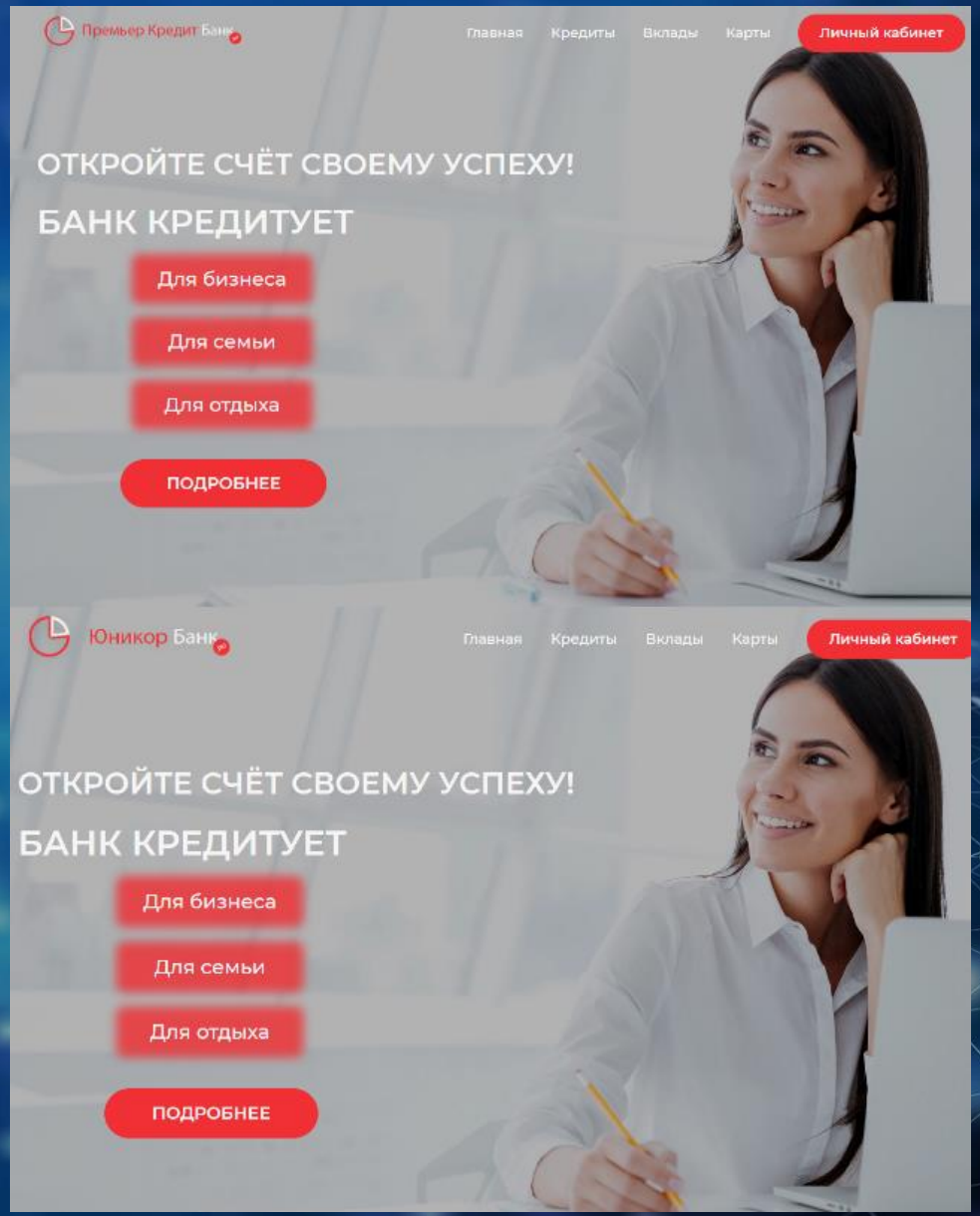
ФИШИНГ

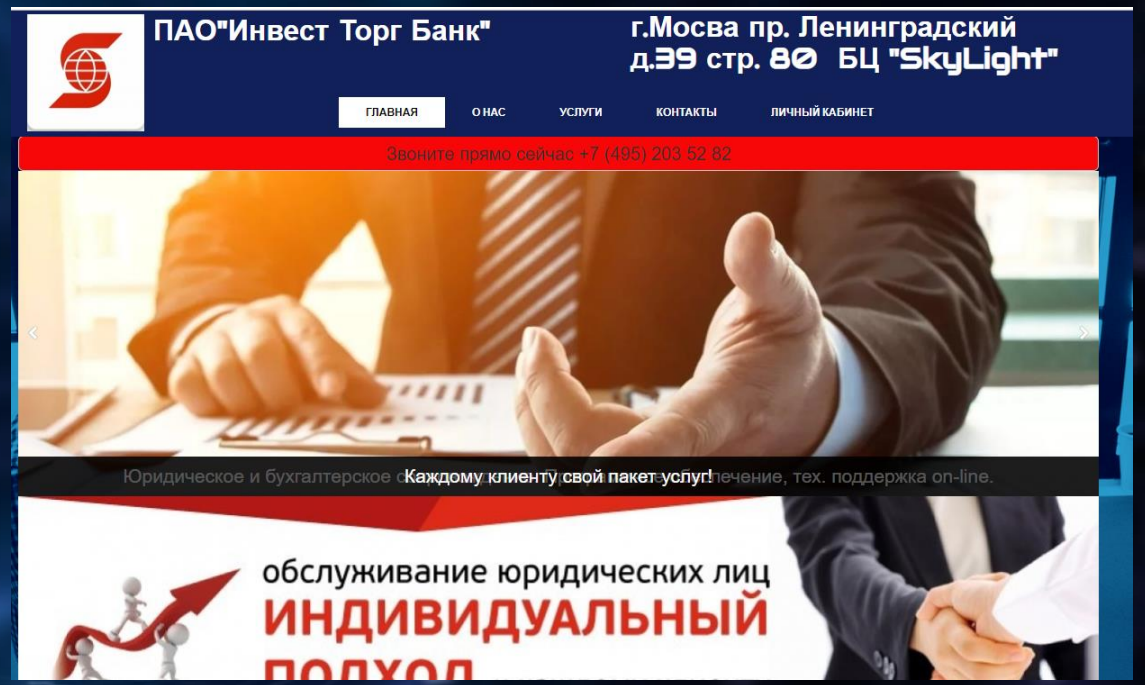

https://toaz.ru
ТОЛЬЯТТИАЗОТ
Поиск по сайту
О компании
Продукция
Инвесторам
Социальная ответственность
Пресс-центр
Работа и карьера
Экология — наш главный приоритет
Тольяттиазот считает своим долгом сохранять благоприятную экологическую обстановку и создавать безопасные условия проживания в окружающих районах.
НОВОСТИ
ПАО «ТОАЗ» в 2018 году сократил выбросы загрязняющих веществ в атмосферу до 2,47 тыс. тонн, что на 60% ниже показателя, зафиксированного годом ранее (4,19
Совет директоров ПАО "ТОАЗ" назначил дату проведения годового общего собрания акционеров общества.
ТОЛЬЯТТИАЗОТ СЕГОДНЯ
ПАО «Тольяттиазот» является одним из крупнейших предприятий в химической промышленности России. Признанный лидер отрасли в стране и за рубежом.
960 тыс. тонн карбамида в год
70 тыс. тонн углекислоты
3 млн тонн жидкого аммиака
ПАО «Тольяттиазот» входит в число 200 крупнейших компаний страны

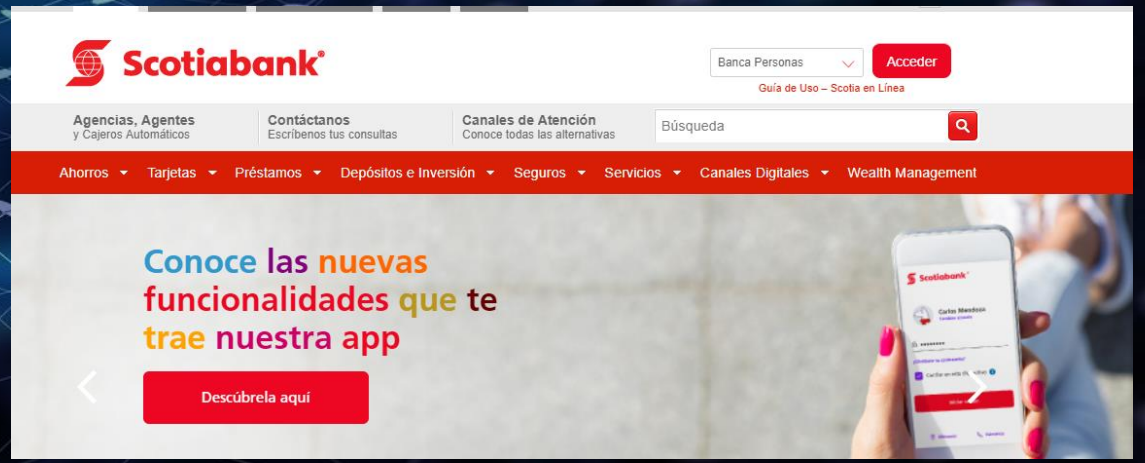

https://toaz.pw
ТОЛЬЯТТИАЗОТ
Поиск по сайту
О компании
Продукция
Инвесторам
Социальная ответственность
Пресс-центр
Работа и карьера
Экология — наш главный приоритет
Тольяттиазот считает своим долгом сохранять благоприятную экологическую обстановку и создавать безопасные условия проживания в окружающих районах.
НОВОСТИ
Тольятти, 17 октября 2018 г. – ПАО «Тольяттиазот», крупнейший производитель аммиака в России, провел торжественную церемонию начала строительства агрегата
В Международный год Периодической системы химических элементов – с ПАО «Тольяттиазот» и Российским химическим обществом им. Д.И. Менделеева.
ТОЛЬЯТТИАЗОТ СЕГОДНЯ
ПАО «Тольяттиазот» является одним из крупнейших предприятий в химической промышленности России. Признанный лидер отрасли в стране и за рубежом.
960 тыс. тонн карбамида в год
70 тыс. тонн углекислоты
3 млн тонн жидкого аммиака
ПАО «Тольяттиазот» входит в число 200 крупнейших компаний страны


toaz.pw
kckk.ru
uralechem.com
toaoz.com
alupro.pro
afinpz.ru
pkz1.net
min-udo.org
agrocenter-eurochem.info
agrocentr-eurochem.cc
metallotreid.ru

???


Премьер Кредит Банк
Главная
Кредиты
Вклады
Карты
Личный кабинет
ОТКРОЙТЕ СЧЁТ СВОЕМУ УСПЕХУ!
БАНК КРЕДИТУЕТ
Для бизнеса
Для семьи
Для отдыха
ПОДРОБНЕЕ
Юникор Банк
Главная
Кредиты
Вклады
Карты
Личный кабинет
ОТКРОЙТЕ СЧЁТ СВОЕМУ УСПЕХУ!
БАНК КРЕДИТУЕТ
Для бизнеса
Для семьи
Для отдыха
ПОДРОБНЕЕ


ПАО"Инвест Торг Банк"
г.Мосва пр. Ленинградский
д.39 стр. 80 БЦ "SkyLight"
ГЛАВНАЯ
О НАС
УСЛУГИ
КОНТАКТЫ
ЛИЧНЫЙ КАБИНЕТ
Звоните прямо сейчас +7 (495) 203 52 82
Каждому клиенту свой пакет услуг!
обслуживание юридических лиц
ИНДИВИДУАЛЬНЫЙ


Scotiabank
Banca Personas
Acceder
Guía de Uso – Scotia en Línea
Agencias, Agentes
y Cajeros Automáticos
Contáctanos
Escríbenos tus consultas
Canales de Atención
Conoce todas las alternativas
Búsqueda
Ahorros
Tarjetas
Préstamos
Depósitos e Inversión
Seguros
Servicios
Canales Digitales
Wealth Management
Conoce las nuevas
funcionalidades que te
trae nuestra app
Descúbrela aquí

Реклама противоправных услуг

УСЛОВИЯ ДЛЯ ПОЛУЧЕНИЯ ПОМОЩИ 📌

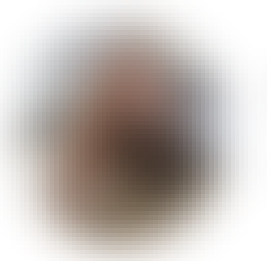
———————————————————

Доброго времени суток,уважаемые клиенты. Хотелось бы для начала представиться, я являюсь сотрудником одного из крупнейших банков Российской Федерации, занимаю руководящую должность. Мы оказываем помощь всем гражданам на территории РФ,требования к заемщикам одно: Возраст от 18 лет до 65 лет. Мы работаем с ситуациями любой сложности, как с положительной так и с отрицательной кредитной историей, работаем с просроченной задолженностью, оформляем граждан при наличии вынесенных судебных решений. Грубо говоря, нас не интересует ваша кредитная история, наличие официального дохода, судимости и пр.

Мы не брокеры! Мы не занимаемся рассылками анкет по банкам, мы работаем только с одним банком!Работая с нами отказ невозможен! Мы гарантируем вам 100% положительное решение!

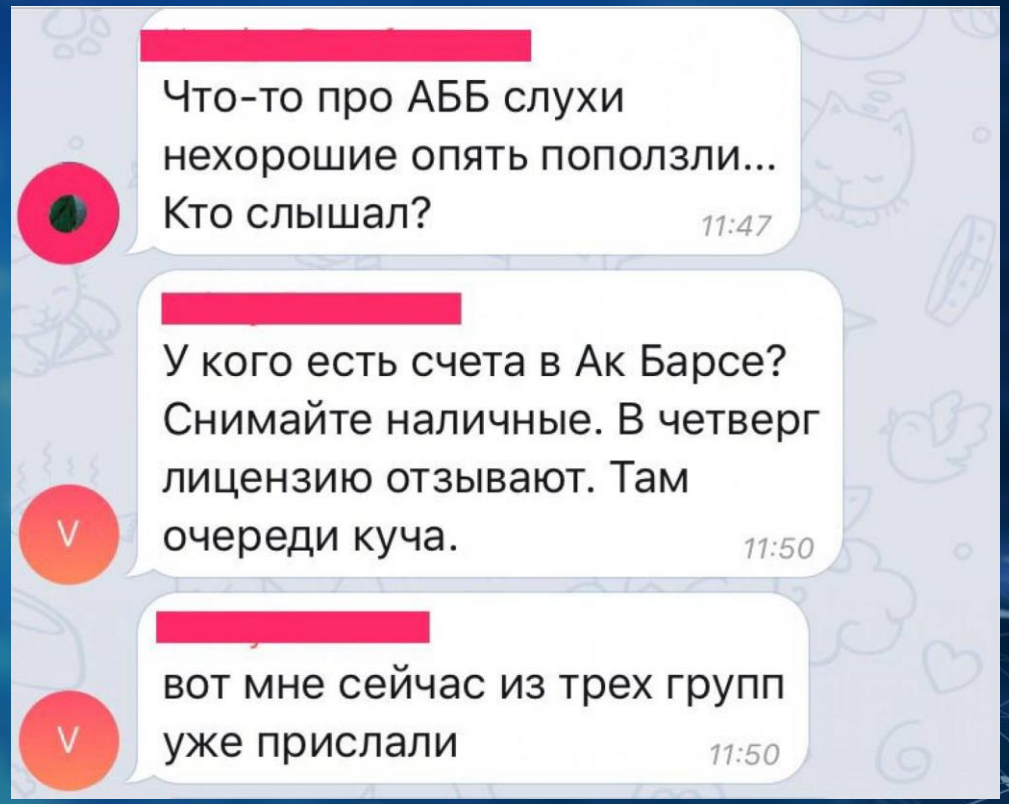
Суммы с которыми мы работаем: от 300.000 рублей до 6.000.000 рублей (свыше рассматриваем индивидуально).

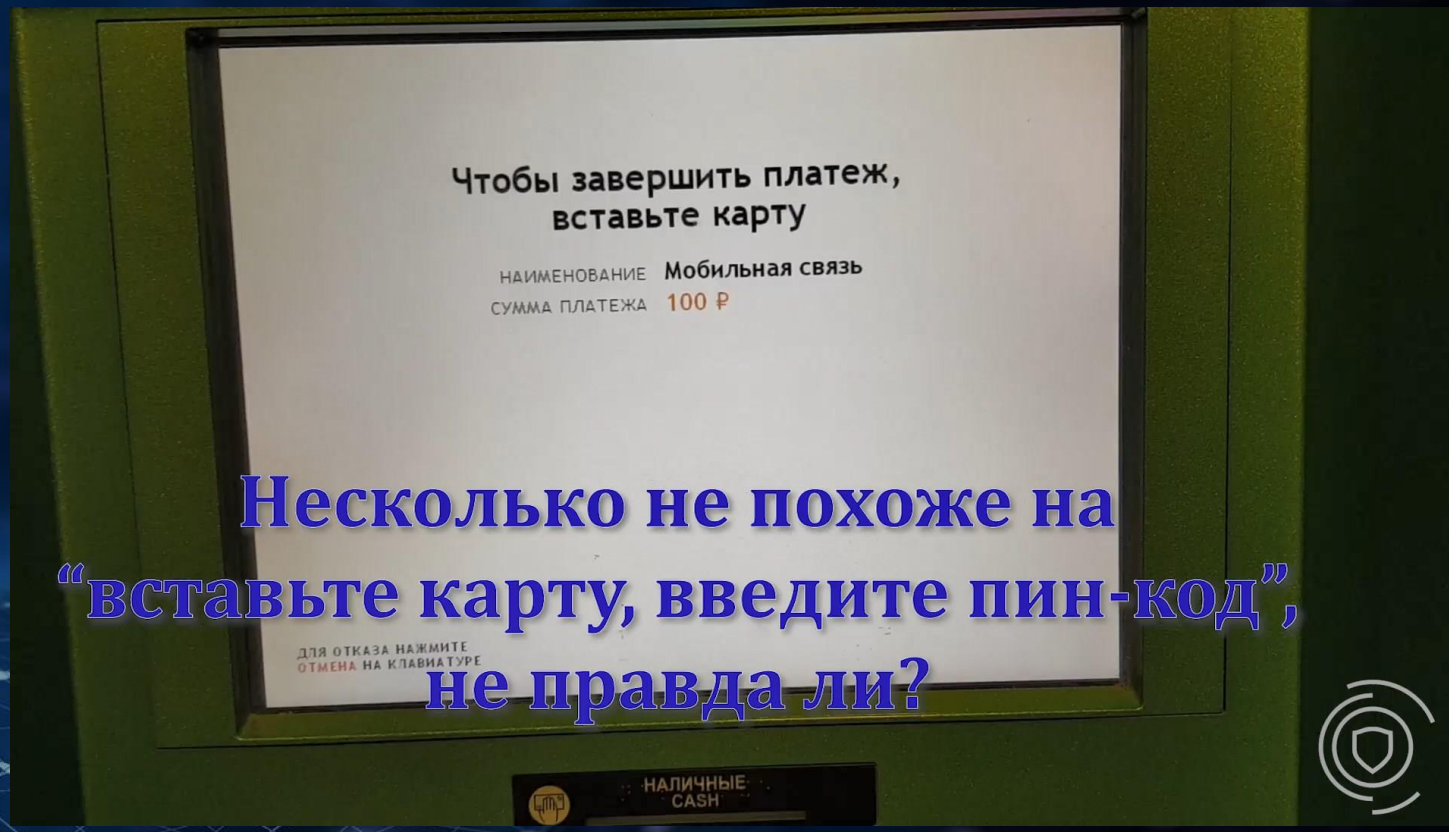
Вербовка сотрудников



СОДЕЙСТВИЕ в Открытие счёта в МОСКВЕ ИЗ ПЕРВЫХ РУК НЕ ПОСРЕДНИК!
А так же в Регионах по запросу (в т ч организациям которые в блоке других банках 550 115фз)с директором и без ,закрытие , пробив остатка счёта,выписки со счёта,вывод средств без пометок на контрагента А так же Приглашаем к сотрудничеству работников банковской сферы для совместной плодотворной работы в направлении открытия расчетных счетов . Мы гарантируем стабильный поток клиентов, большой объем продаж сопутствующих доп. услуг , хорошее вознаграждение
Все конфиденциально!

PR-атаки





Несколько не похоже на “вставьте карту, введите пин-код”, не правда ли?

Первое сообщение в VK – 7 мая

Пик сообщений – 18-20 мая

Что такое ETHIC?

Сервис ETHIC предназначен для выявления на ранних стадиях цифровых угроз бизнесу в глобальных информационных и телекоммуникационных сетях, что позволяет своевременно реагировать на угрозы, не допуская наступления негативных последствий или минимизируя их.

Какие задачи решает ETHIC?

- снижение рисков информационной, экономической безопасности и репутационных потерь
- предотвращение неправомерного использования бренда
- выявление утечек информации, компрометации учетных записей, мобильного фрода
- защита от фишинга
- противодействие мошенникам
- защита от социальной инженерии
- выявление и пресечение информационных атак
- проверка контрагентов

Источники данных ETHIC

Ресурсы DarkNet – анонимные сайты и форумы, размещенные в распределенных сетях Tor, i2p

Реестры доменных имен

«Черные списки» (реестр дисквалифицированных лиц, иностранных агентов, санкционные списки, перечень террористических организаций и т.п.)

Ресурсы Deep Web - веб-страницы «Всемирной паутины», неиндексируемые поисковыми системами

Государственные информационные системы и интеграторы данных

Социальные сети (Вконтакте, Facebook, Instagram, Мой Мир, Twitter, Одноклассники) и мессенджеры (Skype, Telegram и т.д.)

Базы данных публичных утечек

Сервисы поиска работы (hh.ru, avito.ru и т.д.)

Магазины мобильных приложений (Google Play Market, Apple Store, Windows Store, Яндекс.Store)

Торговые площадки (avito.ru, youla.ru и аналоги)

Порядок работы сервиса

МОНИТОРИНГ

Автоматический анализ источников вне периметра компании: от соцсетей до ресурсов DarkNet

ОЦЕНКА

Аналитическая экспертиза уровня опасности и определение тактики реагирования

ОПОВЕЩЕНИЕ

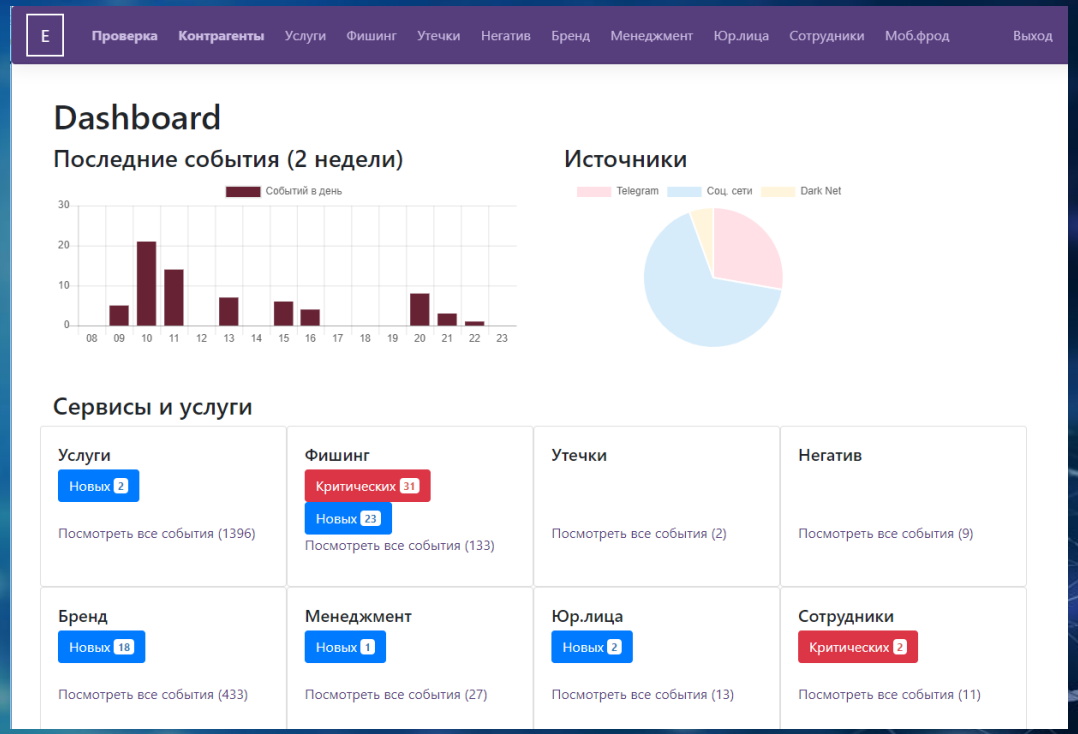
Отправка предупреждений об угрозах для бизнеса или инцидентах через специальный веб-портал

РЕАГИРОВАНИЕ

Блокировка источников, изменение технических настроек сервисов, проведение расследования

Портал ETHIC

Работа сервиса реализована на базе собственного облачного решения.
Взаимодействие заказчика сервисом ETHIC осуществляется по модели SaaS* через веб-интерфейс



Преимущества модели SaaS

- отсутствие необходимости дополнительной интеграции сервиса в инфраструктуру заказчика
- отсутствие необходимости приобретения и установки дополнительного оборудования
- возможность гибкой настройки под потребности заказчика
- заботы о поддержании непрерывного функционирования сервиса и его модернизации полностью лежат на стороне провайдера услуги

*Software as a service – программное обеспечение как услуга

Модули ETHIC

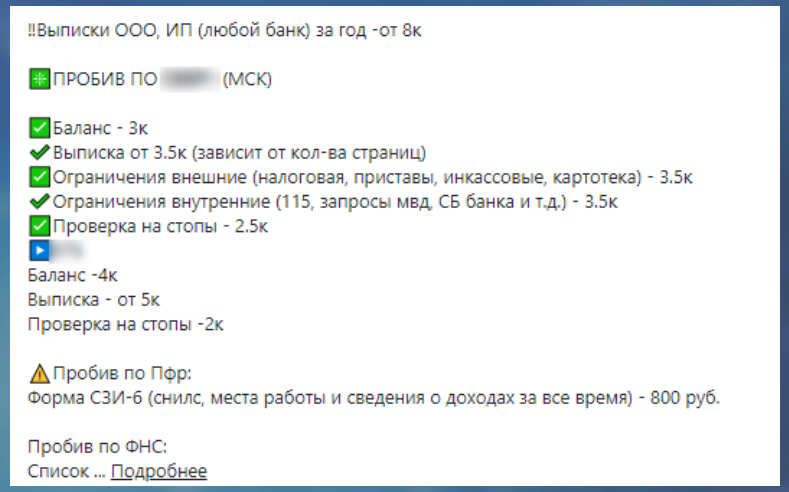
В состав сервиса входит 12 модулей:

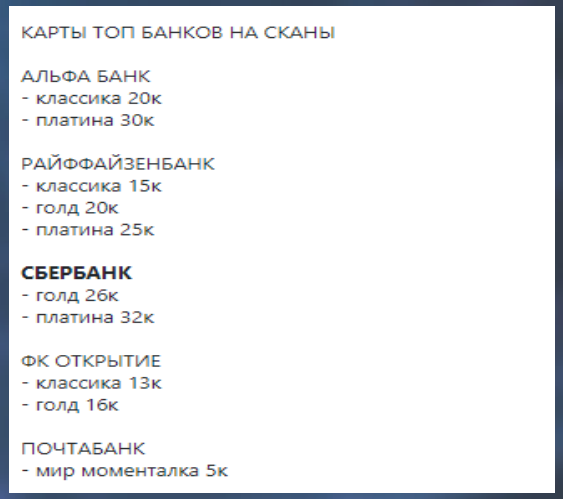
- УСЛУГИ
- ФИШИНГ
- УТЕЧКИ
- НЕГАТИВ
- БРЕНД
- МЕНЕДЖМЕНТ
- СОТРУДНИКИ
- ЮР. ЛИЦА
- МОБИЛЬНЫЙ ФРОД
- КОНТРАГЕНТЫ
- ПРОВЕРКА
- РЕПОЗИТОРИИ

Модульность сервиса позволяет заказчику получать услуги в требуемом ему объеме, избегая тем самым лишних затрат

Модуль «Услуги»

Выявленные события





Анализ угрозы:

- вероятное наличие инсайдера в организации
- риски для клиентов
- риски утечки конфиденциальной информации
- репутационные риски
- риски санкций со стороны регулятора

Действия со стороны «Инфосекьюрити»*:

- установление лица, разместившего объявление
- проведение «проверочной закупки»
- блокирование аккаунтов и удаление сообщений
- подготовка материалов для проведения внутренней проверки или направления в правоохранительные органы

Действия со стороны заказчика:

- проведение внутренней проверки
- выявление сотрудников, причастных к противоправной деятельности
- обращение в правоохранительные органы (при необходимости)
- совершенствование мер внутреннего контроля на основе результатов анализа инцидента

Результат:

- устранение каналов утечки информации
- выявление неблагонадежных сотрудников
- снижение финансовых и репутационных рисков

*В рамках услуги «Оперативное реагирование на инциденты»

Модуль «Фишинг»

Выявленные события

[redacted]

Добавлен 2019-05-03

Изменен 2019-05-06

IP
87.236.16.134

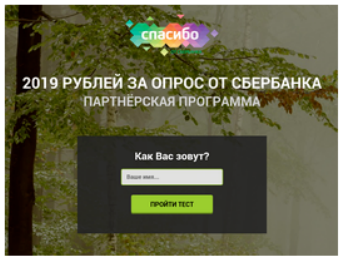
MX

NS
ns2.beget.com
ns1.beget.pro
ns2.beget.pro
ns1.beget.ru
ns2.beget.ru
ns1.beget.com

введите, спасибо, опрос, кцию, карты, своих, лучит, ответьте, вопросы, усовершенствования, услуг, качества, [redacted], если, бонус, номер, клиентов, далее, [redacted], получите, понравилось, приходилось, пройти, поступит, завершить, программа, уважением, рубл, внимательны, будьте, пожалуйста

Изменил whois = domain: [redacted].RU
nserver: ns1.beget.com.
nserver: ns1.beget.pro.
nserver: ns2.beget.com.
nserver: ns2.beget.pro.
state: REGISTERED, NOT DELEGATED, UNVERIFIED
person: Private Person
registrar: BEGET-RU
admin-contact: whois.beget.com
created: 2019-05-01T14:34:11Z
paid-till: 2020-05-01T14:34:11Z
free-date: 2020-06-01
source: TCI (было domain: [redacted].RU
nserver:

domain: [redacted].RU
nserver: ns1.beget.com.
nserver: ns1.beget.pro.
nserver: ns2.beget.com.
nserver: ns2.beget.pro.
state: REGISTERED, NOT DELEGATED, UNVERIFIED
person: Private Person
registrar: BEGET-RU
admin-contact: whois.beget.com
created: 2019-05-01T14:34:11Z
paid-till: 2020-05-01T14:34:11Z
free-date: 2020-06-01
source: TCI



Действия со стороны «Инфосекьюрити»*:

- идентификация владельца ресурса, хостера и регистратора домена
- формирование уведомления о нарушении прав заказчика
- составление и отправка обоснованной претензии администратору сайта
- направление жалобы хостинг-провайдеру и регистратору доменного имени
- обращение к поисковым системам для удаления ресурса из поисковой выдачи
- работа с регуляторами по имеющимся претензиям со стороны правообладателей

Действия со стороны заказчика:

- согласование перечня необходимых действий
- предоставление доверенности
- предоставление необходимых документов, подтверждающих права на интеллектуальную собственность и средства индивидуализации

Результат:

- блокирование фишингового ресурса
- снижение финансовых и репутационных рисков
- повышение лояльности клиентов

*В рамках услуги «Оперативное реагирование на инциденты»

Модуль «Утечки»

Выявленные события

Учетная запись	vk.com, Anti Public Combo List, Exploit.In		og[redacted]@[redacted].ru	Компрометация учетной записи "Ольга[redacted]"
Документы	https://vk.com/doc75232830_476534394	 vk.com		Документ содержащий подпись и печать официального представителя партнера Банка и конфиденциальные данные клиента.

Анализ угрозы:

- информация может использоваться для атаки на организацию
- персональные данные клиента могли оказаться в общем доступе по вине сотрудников организации

Действия со стороны «Инфосекьюрити»*:

- установление источника компрометации данных
- установление лица, разместившего информацию
- анализ распространения информации (количество скачиваний и т.д.)
- блокирование аккаунтов и удаление сообщений (при необходимости)

Действия со стороны заказчика:

- оценка возможного вреда от распространения информации
- защита скомпрометированных учетных записей

Результат:

- выявление сотрудников, допустивших утечку
- недопущение неправомерного использования конфиденциальной информации
- предотвращение возможных атак на организацию
- совершенствование регламентов обеспечения ИБ

*В рамках услуги «Оперативное реагирование на инциденты»

Модули ETHIC

ЮРИДИЧЕСКИЕ ЛИЦА

Сведения о продаже юридических лиц и ИП. Данные лица могут быть незаконно использованы в качестве фиктивных контрагентов Заказчика или иметь расчетные счета, используемые для легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и иной нелегальной деятельности

РЕПОЗИТОРИИ

Мониторинг GitHub, Pastebin и прочих ресурсов на предмет выявления потенциально опасного кода, в т.ч. вредоносных программ, скриптов и эксплойтов, нацеленных на инфраструктуру или продукты Заказчика

КОНТРАГЕНТЫ (скоринг юридического лица)

Автоматизированный поиск и анализ информации о юридическом лице в открытых источниках, а также в собственном реестре неблагонадежных компаний.

Модуль позволяет выявлять не только фирмы-однодневки, но и выставленные на продажу юридические лица, имеющие долгую и хорошую репутацию, необходимые лицензии и коды ОКВЭД, не замеченные ранее в участии в сомнительных схемах (то есть успешно проходящие традиционную комплаенс-проверку)

ПРОВЕРКА

Получение сведений о физических, юридических лицах или имуществе на основе анализа общедоступных онлайн-источников информации. Автоматизированный анализ сведений из государственных реестров, публичных баз данных и иных открытых источников. Формирование отчета занимает от нескольких секунд до двух-трех минут. Возможна пакетная загрузка и обработка массивов данных

ВАЖНО: Модули «Контрагенты» и «Проверка» представляют собой автоматизированные поисково-аналитические системы. Достоверность информации, предоставляемой данными модулями, напрямую зависит от достоверности сведений, содержащихся в соответствующих реестрах и базах данных. Основное назначение модулей – сокращение времени, требуемого на сбор и анализ информации из публичных источников. В случае, если предоставленная в рамках работы модулей информация требуется для принятия ответственного решения, мы рекомендуем заказывать комплексный аналитический отчет

Преимущества ETHIC

- простота работы и автоматизация рабочих процессов
- отсутствие нагрузки на инфраструктуру заказчика
- многоступенчатая верификация угроз опытными аналитиками
- модульность сервиса
- широкий перечень объектов мониторинга
- удобный интерфейс
- гибкость настройки с учетом специфики бизнеса заказчика
- оперативное реагирование на инциденты

У нас есть инструмент… и умелые руки!

БЛАГОДАРЮ ЗА ВНИМАНИЕ

Александр Вураско
ведущий аналитик ГК «Инфосекьюрити»

vurasko@in4security.com
Тел. +7 903 787 17 89