INFOSECURITY
a Softline company

ETHIC

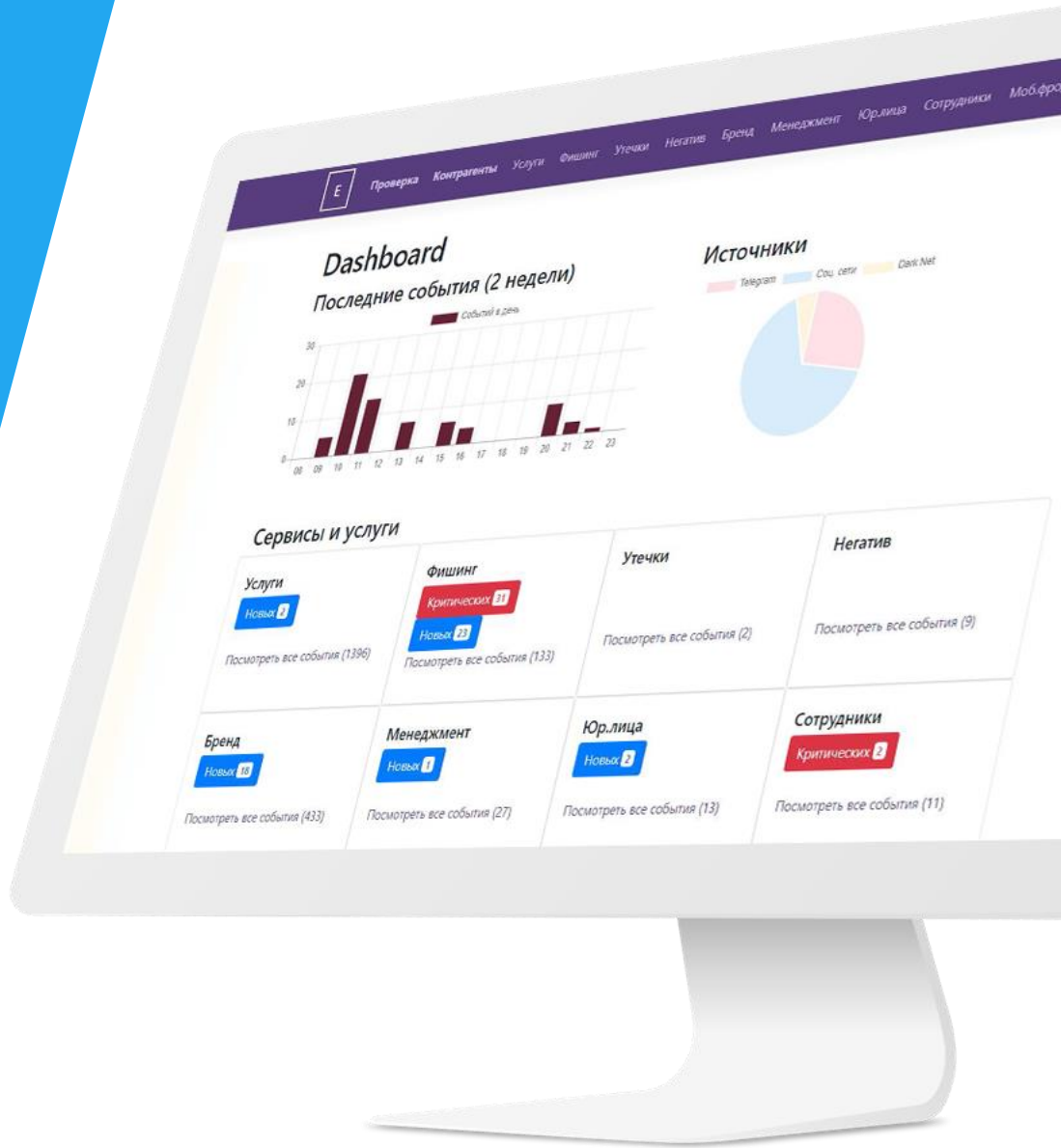
СЕРВИС ВЫЯВЛЕНИЯ УГРОЗ ДЛЯ БИЗНЕСА

Вураско Александр
ведущий аналитик

+7 (499) 677 10 00 доб. 10-4971

+7 (903) 787 17 89

vurasko@in4security.com



ЧТО ТАКОЕ ETHIC?

ВНЕШНИЕ УГРОЗЫ

ВНЕШНИЕ УГРОЗЫ

Решения?.. ETHIC!

ЧТО ТАКОЕ ETHIC?

Сервис ETHIC предназначен для выявления на ранних стадиях цифровых угроз бизнесу в глобальных информационных и телекоммуникационных сетях

КАКИЕ ЗАДАЧИ РЕШАЕТ ETHIC?

- Снижение рисков информационной, экономической безопасности и репутационных потерь
- Выявление утечек информации, компрометации учетных записей
- Предотвращение неправомерного использования бренда
- Выявление и пресечение информационных атак
- Противодействие мошенникам
- Защита от социальной инженерии
- Проверка контрагентов
- Защита от фишинга

ПОРЯДОК РАБОТЫ СЕРВИСА

1 МОНИТОРИНГ

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

2 ОЦЕНКА

Аналитическая экспертиза уровня опасности и определение тактики реагирования

3 ОПОВЕЩЕНИЕ

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

4 РЕАГИРОВАНИЕ

Блокирование источников, изменение технических настроек сервисов, проведение расследования

МОДУЛИ ETHIC

ВЫ САМИ ОПРЕДЕЛЯЕТЕ НЕОБХОДИМЫЙ ОБЪЕМ СЕРВИСА

В СОСТАВ СЕРВИСА ВХОДИТ

10

МОДУЛЕЙ

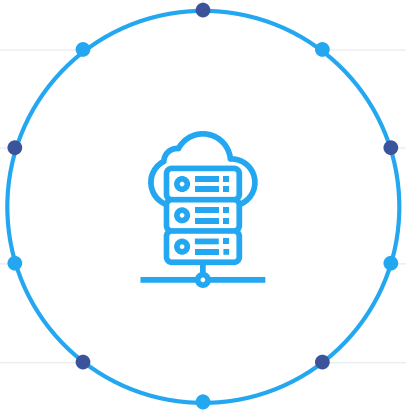
ИСТОЧНИКИ ДАННЫХ ETHIC

Ресурсы DarkNet

«Чёрные списки» и реестры

Социальные сети и мессенджеры

Государственные информационные системы и интеграторы данных



Публичные репозитории и системы управления версиями приложений

Сервисы поиска работы

Ресурсы Deep Web

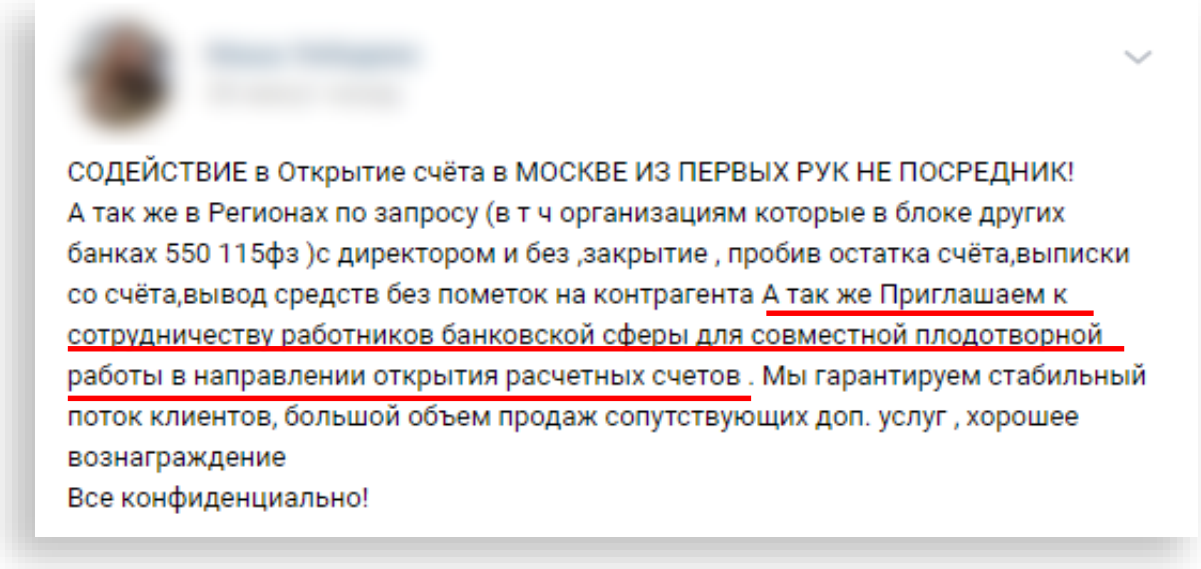
Реестры доменных имен

Торговые площадки

Базы данных публичных утечек

УСЛУГИ

Поиск объявлений о нелегальных услугах, имеющих непосредственное отношение к Заказчику



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!

ВЕКТОРЫ УГРОЗ

- Вербовка сотрудников
- Поиск сообщников
- Реклама противоправных услуг
- Разработка новых криминальных схем
- Обсуждение уязвимостей в бизнес-процессах компаний

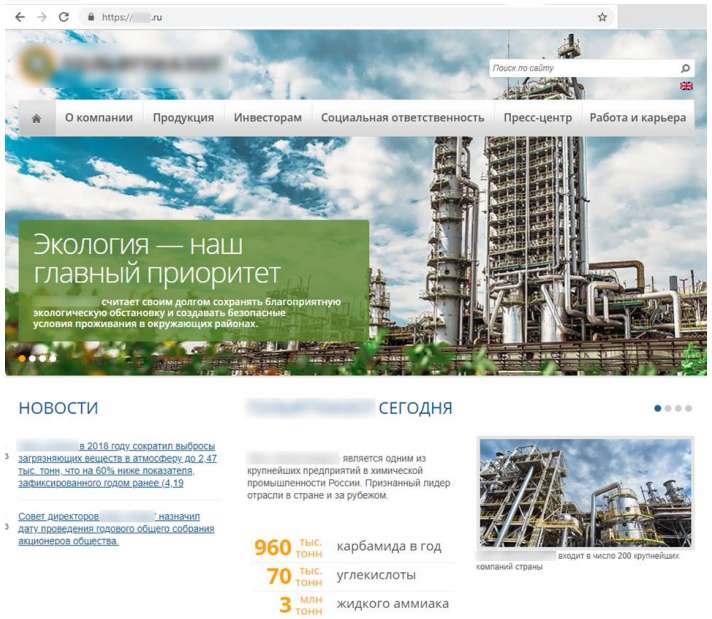
РЕАГИРОВАНИЕ

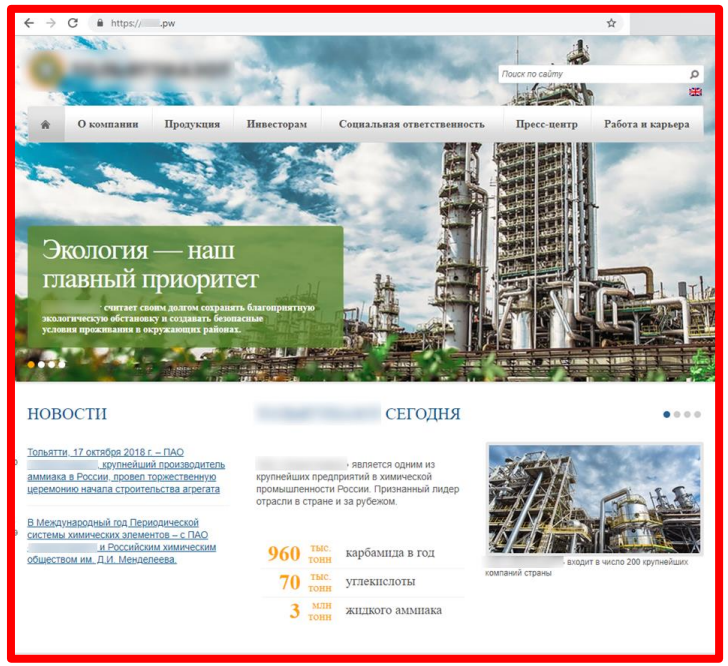
- Установление лиц, разместивших объявления
- Проведение «проверочной закупки»
- Блокирование аккаунтов и удаление сообщений

ДОМЕНЫ

1 ВЫЯВЛЕНИЕ ПОТЕНЦИАЛЬНО-ОПАСНЫХ РЕСУРСОВ ИЛИ ДОМЕНОВ И ОПОВЕЩЕНИЕ ЗАКАЗЧИКА

Анализ пула зарегистрированных доменных имен и выданных SSL-сертификатов





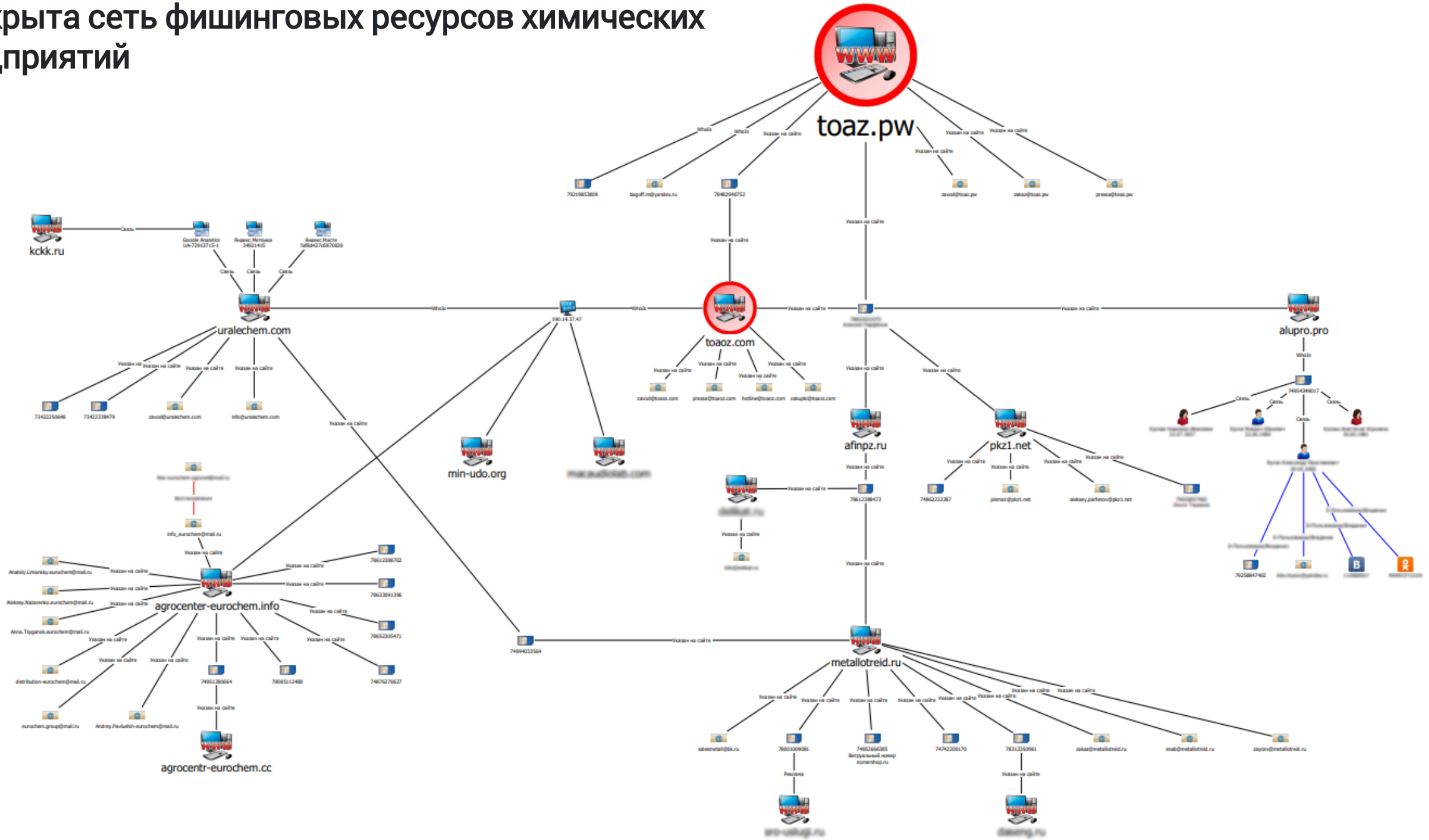
2 РЕАГИРОВАНИЕ НА УГРОЗУ

- Идентификация владельца ресурса
- Блокирование хостинга или домена, удаление из поисковых систем

3 РЕЗУЛЬТАТ

- Снижение финансовых и репутационных рисков
- Повышение лояльности клиентов

Раскрыта сеть фишинговых ресурсов химических предприятий



KAMKABEL.NET

Доменное имя зарегистрировано: **21.07.2019**

Регистратор находится за рубежом, использована услуга анонимной регистрации

Хостинг: **Исландия**

К домену привязан почтовый сервер сервиса ZOHO.EU

УТЕЧКИ

Поиск и выявление информационных активов Заказчика, намеренно или случайно опубликованных в сети Интернет

Компрометация учетных записей сотрудников

alucevitch@****.ru zai1@****.ru olga@pren.****.ru

Размещенный в открытом доступе документ

Телефон (383-43) 2-82-02, факс (383-43) 2-82-01

11.2. АБОНЕНТА

Юридический адрес: ул. К. Маркса, д. 37, г. Бердск, Новосибирская обл, Россия, 633010
Почтовый адрес: ул. К. Маркса, д. 37, г. Бердск, Новосибирская обл, Россия, 633010
Телетайп _____ Телефон (383) 41-21620 телефакс
Расчетный счет 40702810300041000054 в Сибирское ГУ банка России г. Новосибирск
Идентификационный номер ИНН 5445418599 КПП 544501001, БИК 045004001
Коды по ОКВЭД - 10.10.1, ОКПО - 7584544, ОКТМО - _____, ОГРН - 1045404733065
Адрес электронной почты (e-mail) bsk_dk22@mail.ru

ПРИМЕР ДОКУМЕНТА

Данный договор составлен в 2-х экземплярах, один из которых находится у УПОЛНОМОЧЕННОГО ПОСТАВЩИКА, а другой - у АБОНЕНТА.

Подписи:

Гарантирующий поставщик

_____ Е.Г. Кулешов

(доверенность №5-201 от 19.07.2017г.)

Абонент

_____ /Фешина И.М.

РЕЗУЛЬТАТ

1. Недопущение неправомерного использования конфиденциальной информации
2. Предотвращение возможных атак на организацию
3. Совершенствование регламентов обеспечения ИБ

НЕГАТИВ

Выявление публикаций негативного и компрометирующего характера, а также PR-атак

Отрицательные стороны

Контора пытается выглядеть солидной компанией, а по факту внутри присутствует самодурство, неуважение к работникам и т.д.. Текучка кадров у них не спроста. Атмосфера не здоровая, все всего боятся, везде висит дух подглядывания и прослушивания, стукачество. При трудоустройстве первый месяц будешь вкалывать за голый оклад и то который дадут в следующем месяце.. может быть... если не уволишься от безденежья к тому времени))) При увольнении тоже получишь оклад, премиальную часть зарплаты тебе попросту простят - не выплатят -. ты же уволился... Все телефоны прослушиваются, а может и кабинеты. Руководители много твердят как и в других компаниях про якобы командный дух, инновации, но к реальным предложениям относятся болезнено....

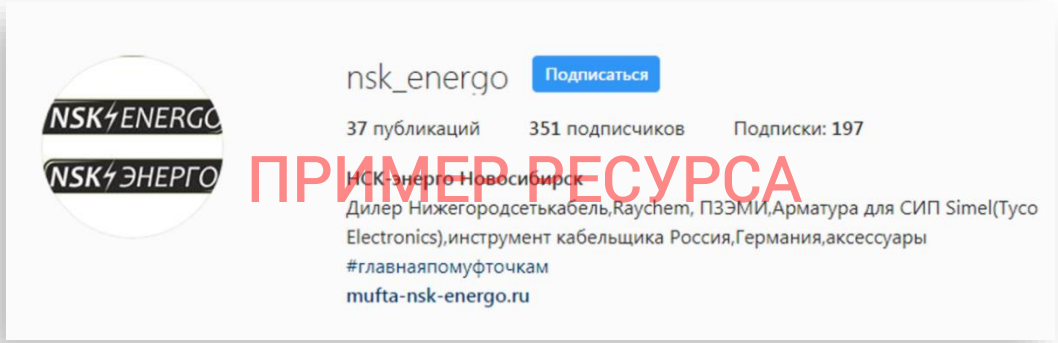
Возможные действия

- Установление источника информации и анализ ее распространения
- Выявление схожих публикаций
- Блокирование аккаунтов и удаление сообщений

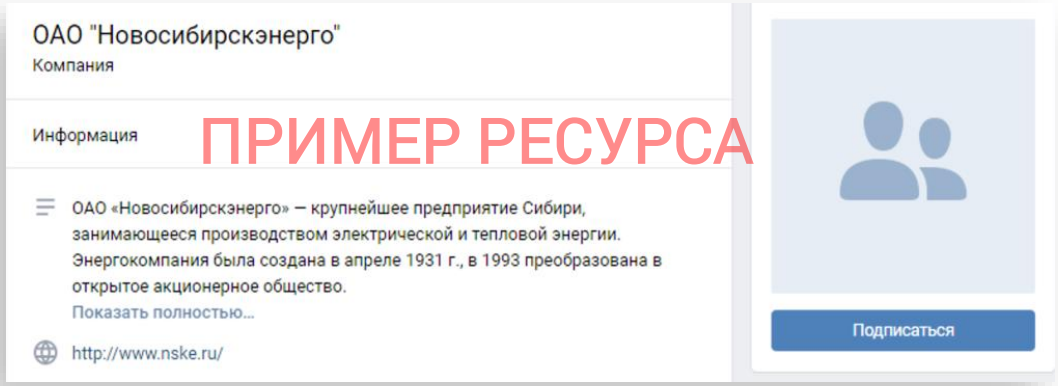
БРЕНД

Выявление неправомерного использования бренда

Использование наименования компании



Использование наименования компании



Возможные действия «Инфосекьюрити»

- Установление владельцев учетных записей
- Составление и отправка претензии
- Юридическое сопровождение

РЕЗУЛЬТАТ

1. Снижение репутационных рисков
2. Повышение лояльности клиентов
3. Выявление атак на организацию, предотвращение мошеннических и иных противоправных схем

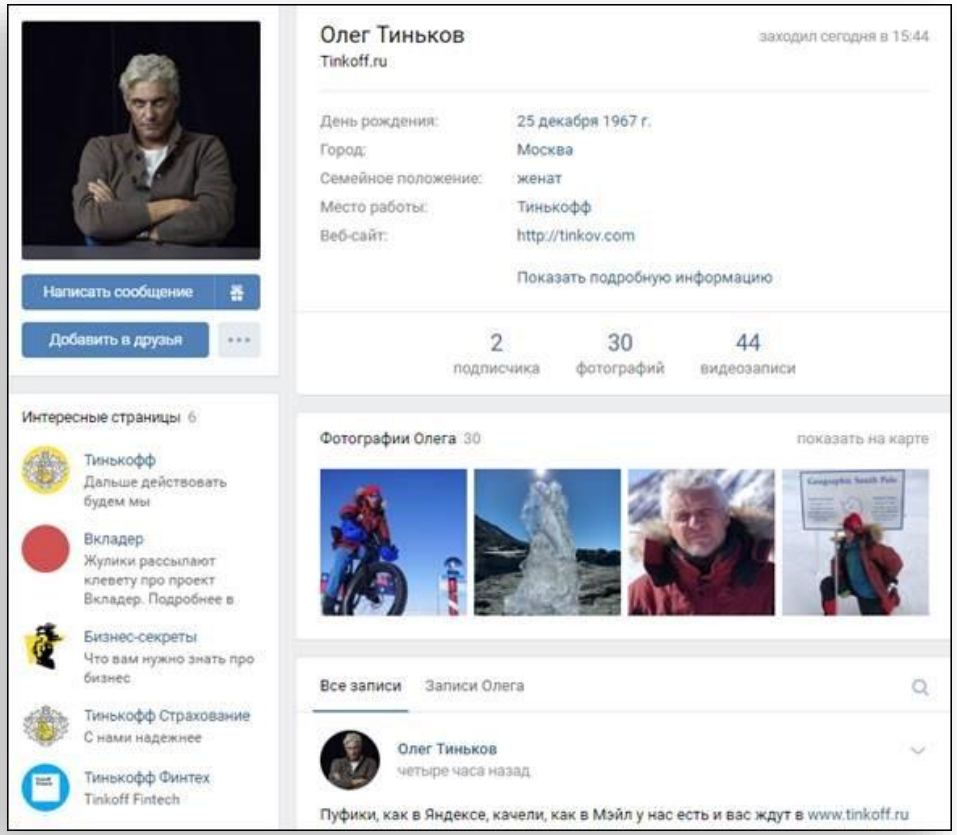
МЕНЕДЖМЕНТ

Выявление поддельных профилей ключевых сотрудников Заказчика в социальных сетях

ФЕЙКОВАЯ СТРАНИЦА ПАВЛА ДУРОВА В 2018

ЭВОЛЮЦИЯ ФОТО ПРОФИЛЯ НА ФЕЙКОВЫХ СТРАНИЦАХ

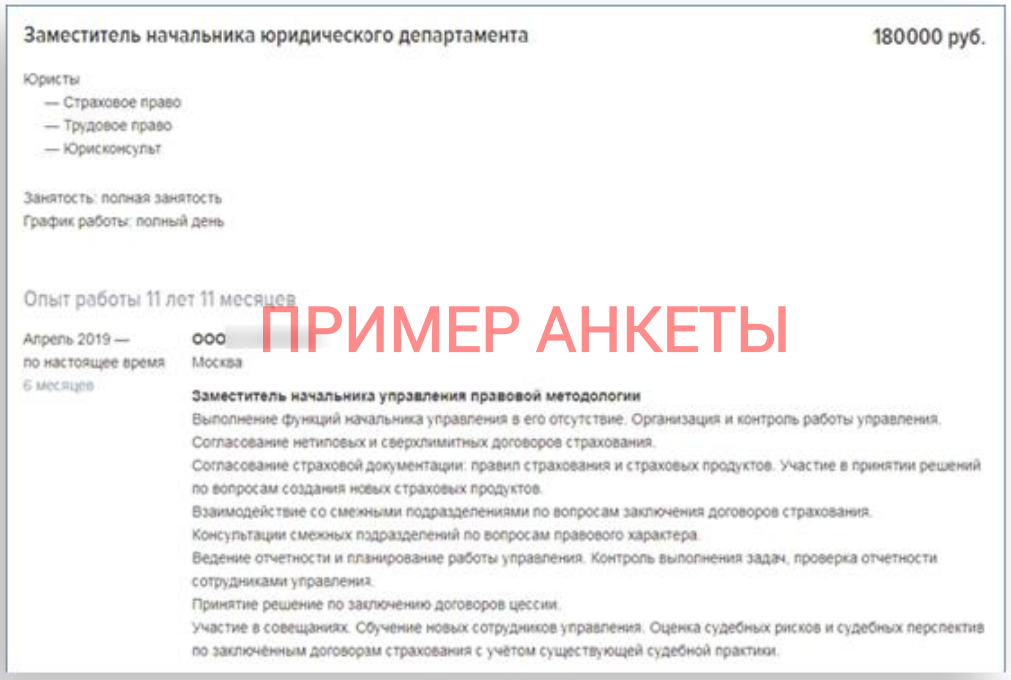
ФЕЙКОВАЯ СТРАНИЦА ОЛЕГА ТИНЬКОВА В 2019



СВОЕВРЕМЕННОЕ ВЫЯВЛЕНИЕ КЛОНА СТРАНИЦЫ ТОП-МЕНЕДЖЕРА ПОЗВОЛЯЕТ ПРЕДОВТРАТИТЬ ФИНАНСОВЫЙ И РЕПУТАЦИОННЫЙ УЩЕРБ

СОТРУДНИКИ

Выявление сотрудников компании Заказчика, находящихся в активном поиске работы



Заместитель начальника юридического департамента 180000 руб.

Юристы
— Страховое право
— Трудовое право
— Юрисконсульт

Занятость: полная занятость
График работы: полный день

Опыт работы 11 лет 11 месяцев

Апрель 2019 — по настоящее время
6 месяцев

ООО
Москва

Заместитель начальника управления правовой методологии
Выполнение функций начальника управления в его отсутствие. Организация и контроль работы управления.
Согласование нетиповых и сверхлимитных договоров страхования.
Согласование страховой документации: правил страхования и страховых продуктов. Участие в принятии решений по вопросам создания новых страховых продуктов.
Взаимодействие со смежными подразделениями по вопросам заключения договоров страхования.
Консультации смежных подразделений по вопросам правового характера.
Ведение отчетности и планирование работы управления. Контроль выполнения задач, проверка отчетности сотрудниками управления.
Принятие решение по заключению договоров цессии.
Участие в совещаниях. Обучение новых сотрудников управления. Оценка судебных рисков и судебных перспектив по заключённым договорам страхования с учётом существующей судебной практики.

ПРИМЕР АНКЕТЫ

Возможные действия Заказчика

- Дополнительная мотивация ценных сотрудников
- Ограничение доступа к конфиденциальной информации
- Аудит условий труда и взаимоотношений в коллективе

РЕЗУЛЬТАТ

1. Предотвращение потери ценных кадров
2. Предотвращение утечки конфиденциальной информации
3. Выявление и устранение конфликтов

ЮРИДИЧЕСКИЕ ЛИЦА

Сведения о нелегальной «продаже» юридических лиц и ИП

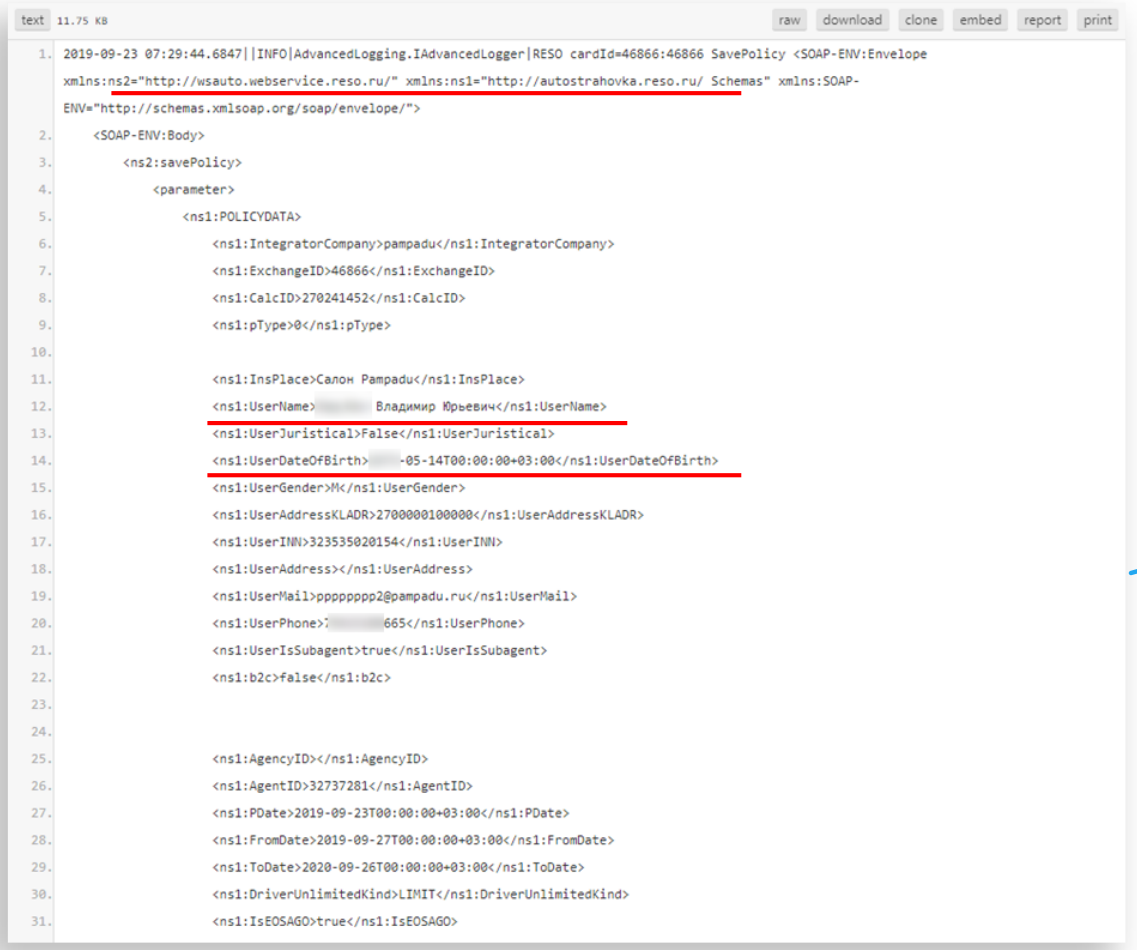
Клиент	Категория	Организация	ИНН	Гендиректор
банк	Продажа Ю.Л. и ИП	ООО "Техно-2000"	6678	Денис Анатольевич ИНН:
банк	Продажа Ю.Л. и ИП	ООО "В.Т.К."	3625	Сергей Александрович
банк	Продажа Ю.Л. и ИП	ООО "Медина"	9723	Елена Александровна ИНН:
банк	Продажа Ю.Л. и ИП	ООО "Дайли"	7702	Эдгар Манвелович
банк	Продажа Ю.Л. и ИП	ООО "Эстер"	9723	Галина Ивановна ИНН:
банк	Продажа Ю.Л. и ИП	ООО ЛАНЖЕРИ	9723	Ольга Игоревна ИНН:

ПРИМЕРЫ ЮР. ЛИЦ

РЕЗУЛЬТАТ

1. Снижение финансовых рисков
2. Предотвращение возможных санкций со стороны регулятора
3. Выявление мошеннических схем

РЕПОЗИТОРИИ



Фрагмент размещенного кода содержит адрес ресурса компании, персональные данные клиентов и прочие сведения

ВЕКТОРЫ УГРОЗ

- Утечки конфиденциальной информации
- Утечки паролей и т.п.
- Информация об инфраструктуре компании и используемых технических решениях
- Размещение вредоносного п/о, предназначенного для атак на компанию

ПРОВЕРКА

Автоматизированная поисково-аналитическая система по трем направлениям
Основное назначение модуля – сокращение времени, требуемого на сбор и анализ информации из публичных источников

ИСТОЧНИКИ:

Поиск по номеру телефона

- SMSC — Проверка доступности абонента
- Поиск на досках объявлений (2016 - н. в.)
- WhatsApp
- Сбербанк-Онлайн
- Viber
- Элекснет — Проверка на наличие кошелька
- Яндекс.Карты
- Google+
- Infobip — Проверка доступности абонента
- Qiwi — Проверка на наличие кошелька
- NumBuster
- Яндекс — Проверка на наличие учетной записи и кошелька Я.Деньги
- TrueCaller

Поиск по email

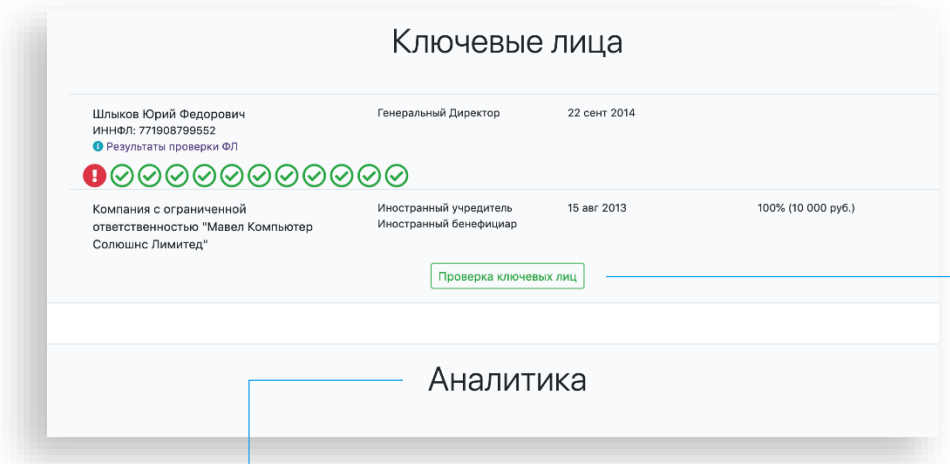
- VK — Поиск профилей
- Skype
- ОК
- РЖД
- Аэрофлот
- Facebook
- Instagram
- Apple
- HH — Поиск резюме

Достоверность информации, предоставляемой данным модулем, напрямую зависит от достоверности сведений, содержащихся в соответствующих реестрах и базах данных

ПРОВЕРКА ЮРИДИЧЕСКОГО ЛИЦА

Автоматизированный скоринг-отчет с анализом общедоступных источников и реестров и выявление вероятных факторов риска

- Сведения о Юрлице
- Общая информация из ЮГРЮЛ
- Государственные закупки
- Исполнительные производства
- Лицензии
- Банкротство
- Реестр договоров 223-ФЗ
- Важные записи в ЕГРЮЛ
- Реестр контрактов 44-ФЗ и 94-ФЗ
- Банковские гарантии
- Приостановление по р/с Госзакупки
- Аффилированные компании
- Недобросовестные поставщики
- Реестр квалифицированных подрядных организаций
- История по ключевым лицам
- Реестр организаций - участников госзакупок
- Реестр договоров на капитальное строительство
- Решения ФНС о предстоящем исключении из ЕГРЮЛ



СКОРИНГ АНАЛИТИКА ЮРИДИЧЕСКОГО ЛИЦА проводится по 20 параметрам

СКОРИНГ-ПРОВЕРКА КЛЮЧЕВЫХ ЛИЦ

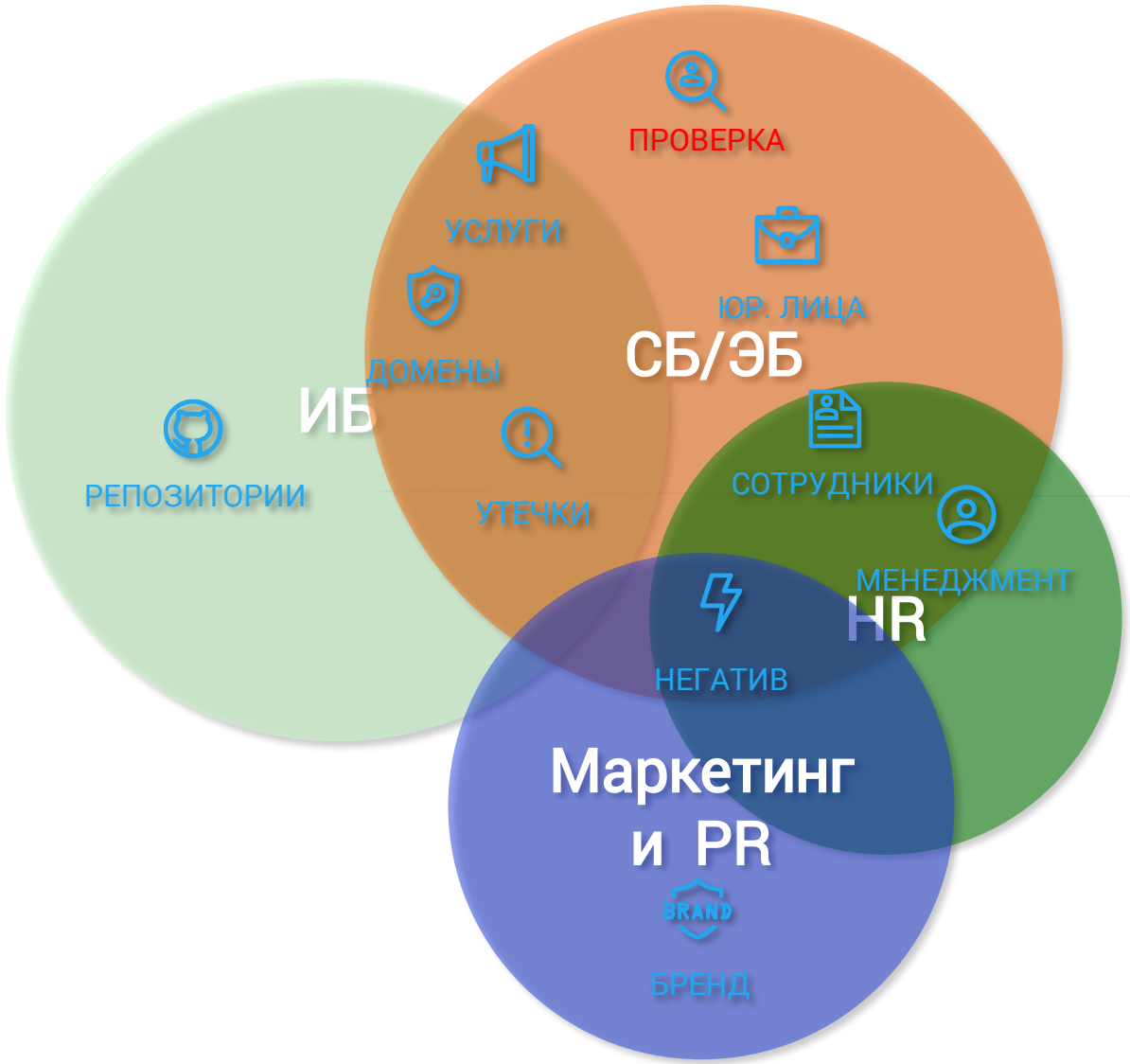
По ФИО+ИНН → проверка по 7 пунктам

1. ФНС - Решения о приостановлении операций по р/с
2. ФНС - Дисквалифицированные лица
3. ФНС - Массовые руководители и учредители
4. ЕФРСБ - Проверка на банкротство
5. ГИС ГМП - поиск задолженности по налогам
6. ГИС ГМП - поиск задолженности по исполнительным производствам
7. ЦБ РФ - проверка по списку отказов

Если ввести дату рождения → проверка еще по 6 пунктам

1. ФНС - проверка статуса плательщика НПД
2. ФСПП - исполнительные производства
3. ЦБ РФ - проверка по списку отказов
4. Росфинмониторинг - проверка по списку террористов
5. ФНП - поиск заложенного имущества физлица
6. МВД - Федеральный розыск

МОДЕЛЬ ВОСТРЕБОВАННОСТИ МОДУЛЕЙ ETHIC



Решаемые задачи со стороны ИБ

- Выявление готовящихся атак
- Получение информации об уязвимостях инфраструктуры
- Предотвращение технических каналов утечек информации
- Выявление компрометации учетных записей

Решаемые задачи со стороны СБ/ЭБ

- Защита активов и проверка контрагентов
- Выявление инцидентов (в том числе на этапе подготовки)
- Выявление инсайдеров в компании
- Проверка сотрудников и кандидатов на работу
- Выявление коррупционных схем, сговора сотрудников и пр.
- Выявление утечек информации , установление виновных и пресечение каналов утечек

Решаемые задачи со стороны HR

- Отслеживание сотрудников, находящихся в поиске работы
- Выявление недобросовестных сотрудников и документирование их деятельности

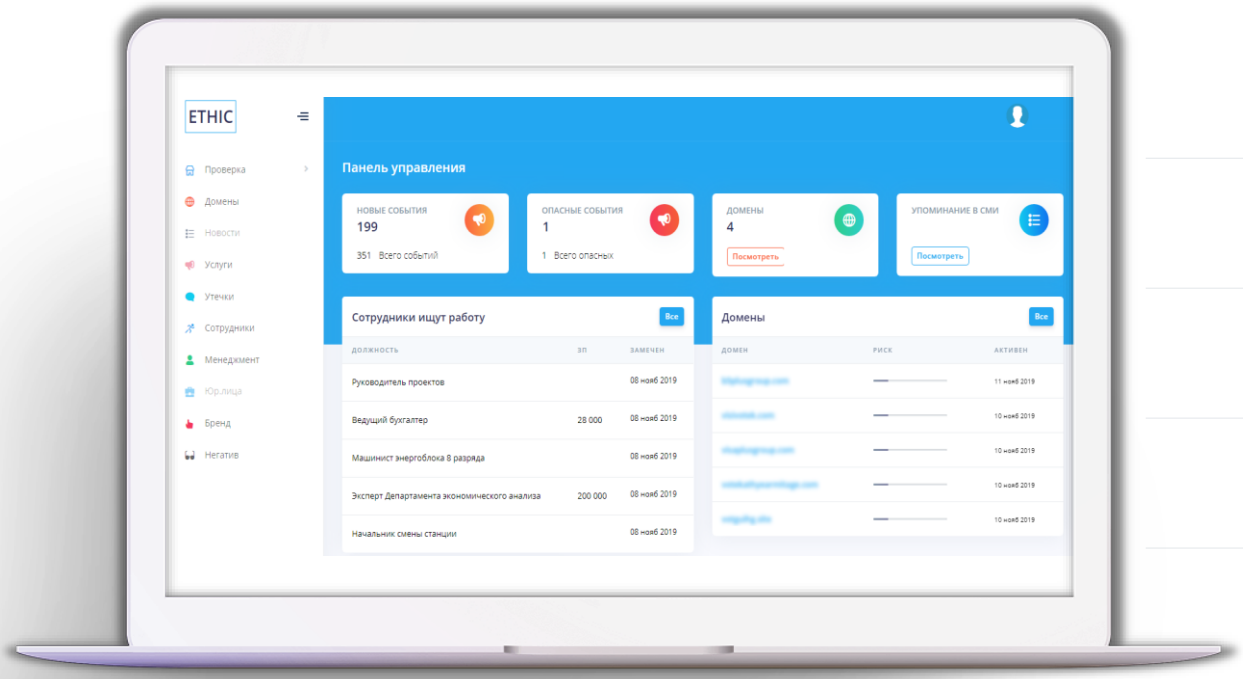
Решаемые задачи со стороны Маркетинга и PR

- Выявление информационных атак
- Выявление злоупотреблений брендом
- Конкурентная разведка

И многое другое…

ПОРТАЛ ETHIC

Работа сервиса реализована на базе собственного облачного решения



Взаимодействие заказчика с 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

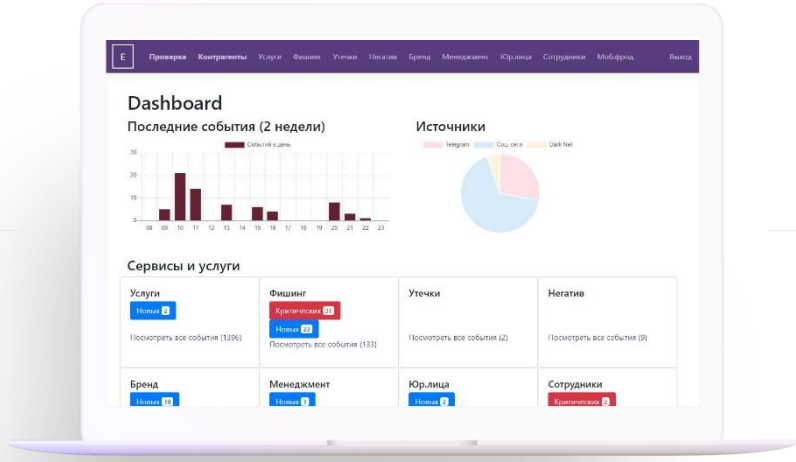
*Software as a service –программное обеспечение как услуга

ПРЕИМУЩЕСТВА ETHIC

Удобный интерфейс

Оперативное реагирование на инциденты

Многоступенчатая верификация угроз опытными аналитиками



Отсутствие нагрузки на инфраструктуру заказчика

Гибкость настройки с учетом специфики бизнеса заказчика

Простота работы и автоматизация рабочих процессов

Широкий перечень объектов мониторинга

Модульность сервиса

INFOSECURITY
a Softline company

ETHIC

СЕРВИС ВЫЯВЛЕНИЯ УГРОЗ ДЛЯ БИЗНЕСА

Вураско Александр
ведущий аналитик

+7 (499) 677 10 00 доб. 10-4971

+7 (903) 787 17 89

vurasko@in4security.com