



Как защититься от кибермошенников: основные онлайн-угрозы и способы противодействия

Андрей Бусаргин

Директор направления Brand Protection



14 лет

опыта предотвращения и расследования киберпреступлений с использованием высоких технологий

1000+

успешных расследований по всему миру, 150 особо сложных уголовных дел

80%

резонансных киберпреступлений в России расследуется с нашим участием

\$300 млн

возвращено клиентам Group-IB благодаря нашей работе



EUROPOL



INTERPOL

Официальный партнёр EUROPOL и INTERPOL



OSCE

Рекомендована Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)



BUSINESS INSIDER

Одна из 7 самых влиятельных компаний в области кибербезопасности по версии Business Insider



Forrester



Gartner

Threat Intelligence от Group-IB – в числе лучших мировых систем по оценке Forrester и Gartner



Угрозы

**Интернет-мошенничество,
неправомерное
использование бренда**

Информационные атаки

Схемы

- Мошеннические сайты, сайты-клоны, фишинг
 - Ложное партнерство
 - Неправомерная реклама
 - Поддельные аккаунты и группы в соцсетях
-
- Направленные бот-атаки против бренда
 - Распространение негатива о бренде и руководстве



Интернет-мошенничество в России



100 млрд
рублей

ежегодный ущерб компаний
в России от неправомерного
использования их бренда

25 тысяч
сайтов

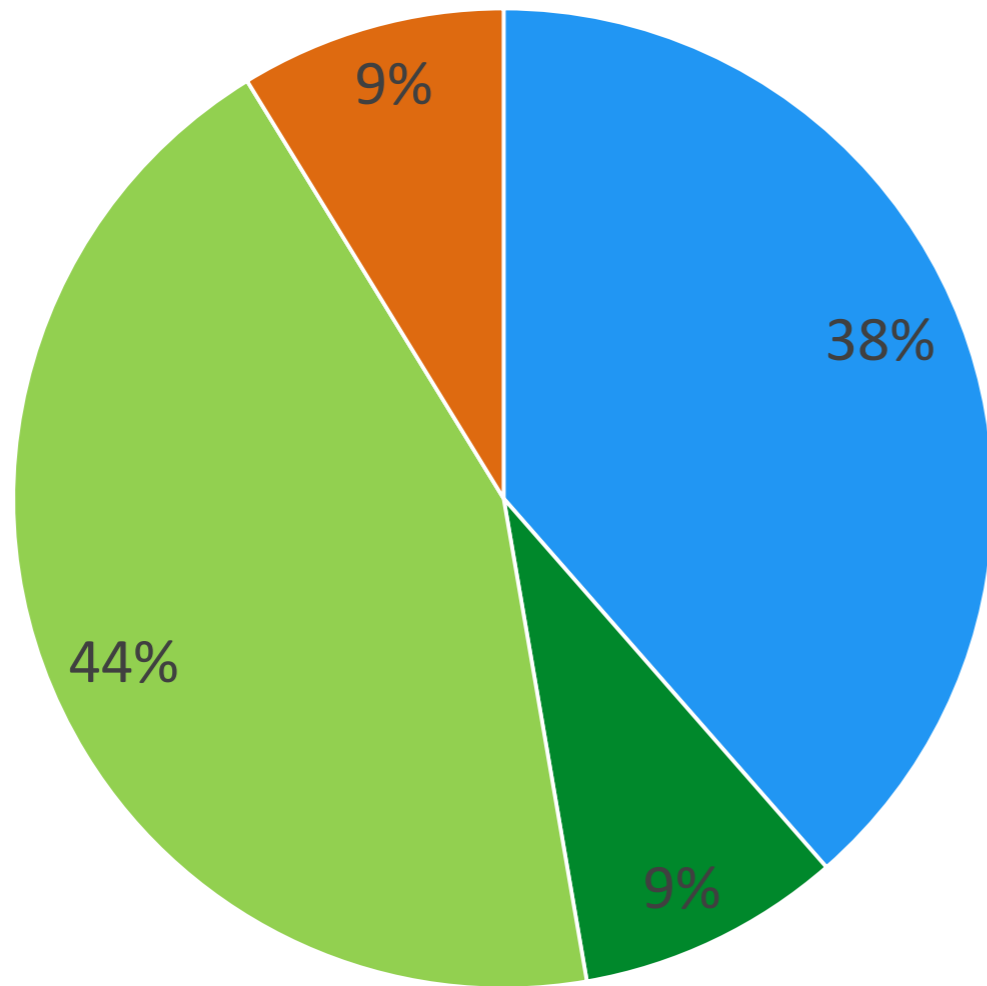
ежедневно создают
мошенники в мире

750 млн
пользователей

в месяц попадают минимум
на один мошеннический сайт



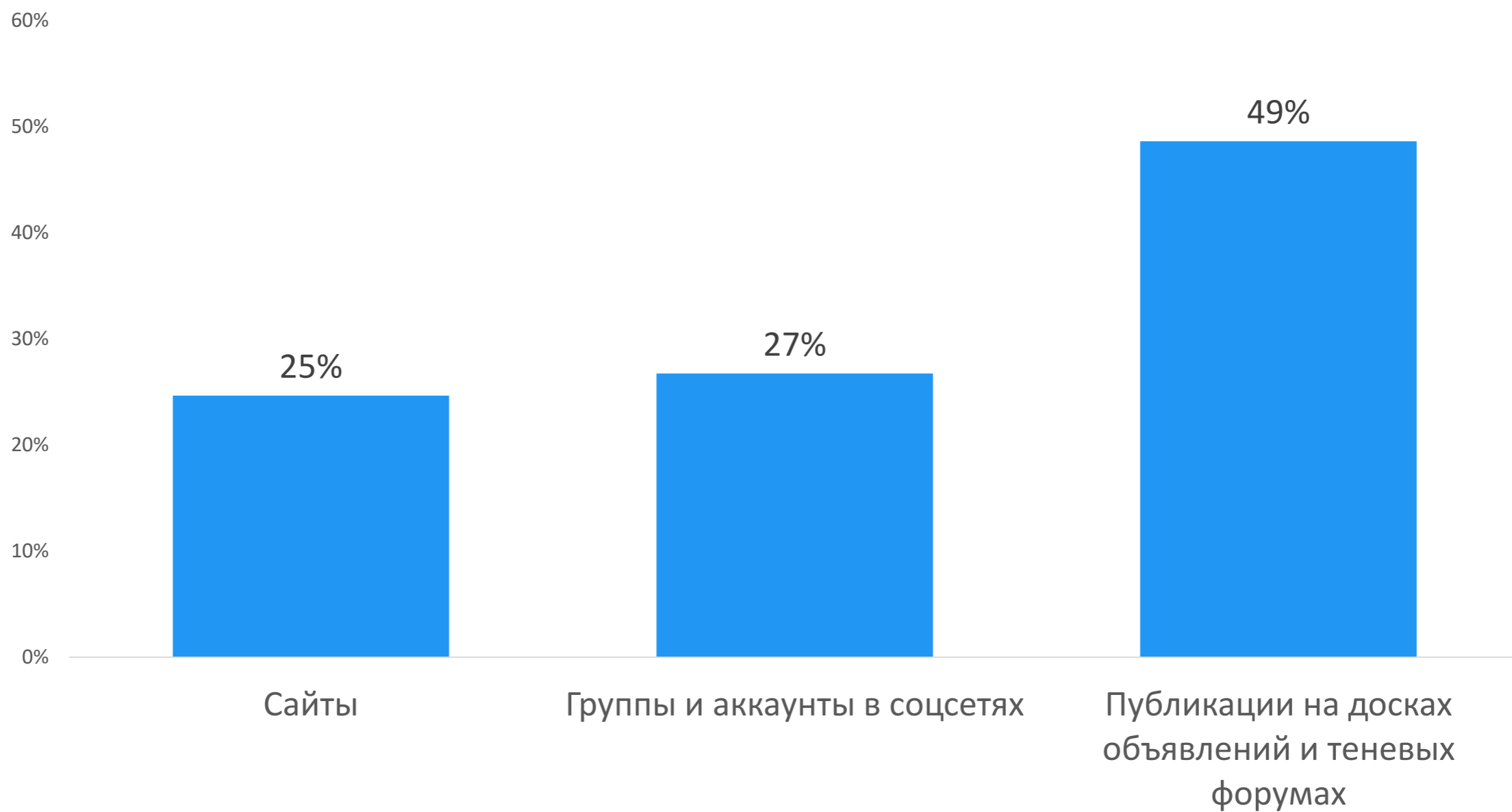
Нарушения в сфере автострахования в 2017 году | GROUP IB



- Продажа бланков ОСАГО
- Продажа электронных ОСАГО
- Продажа диагностических карт ТО онлайн
- Ложное партнерство



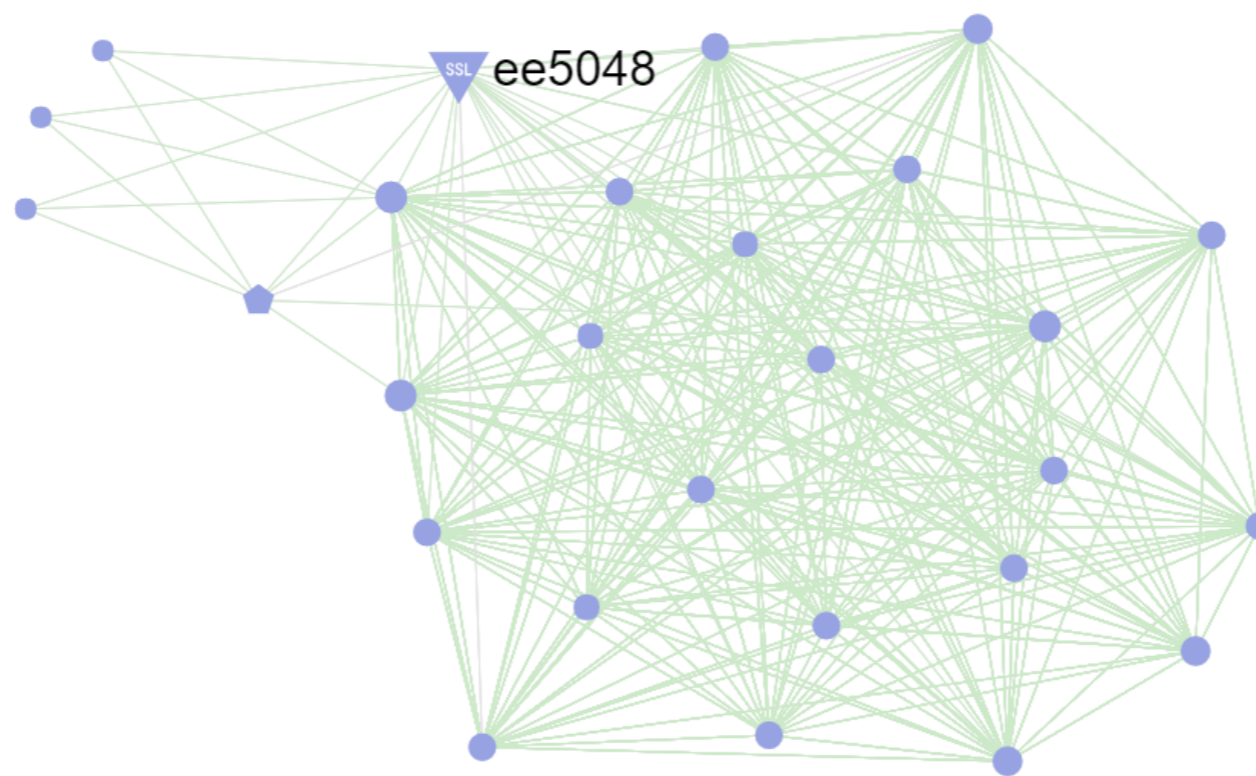
Онлайн-угрозы для страховых компаний



Как действуют онлайн-мошенники



Создание сети мошеннических сайтов одним злоумышленником

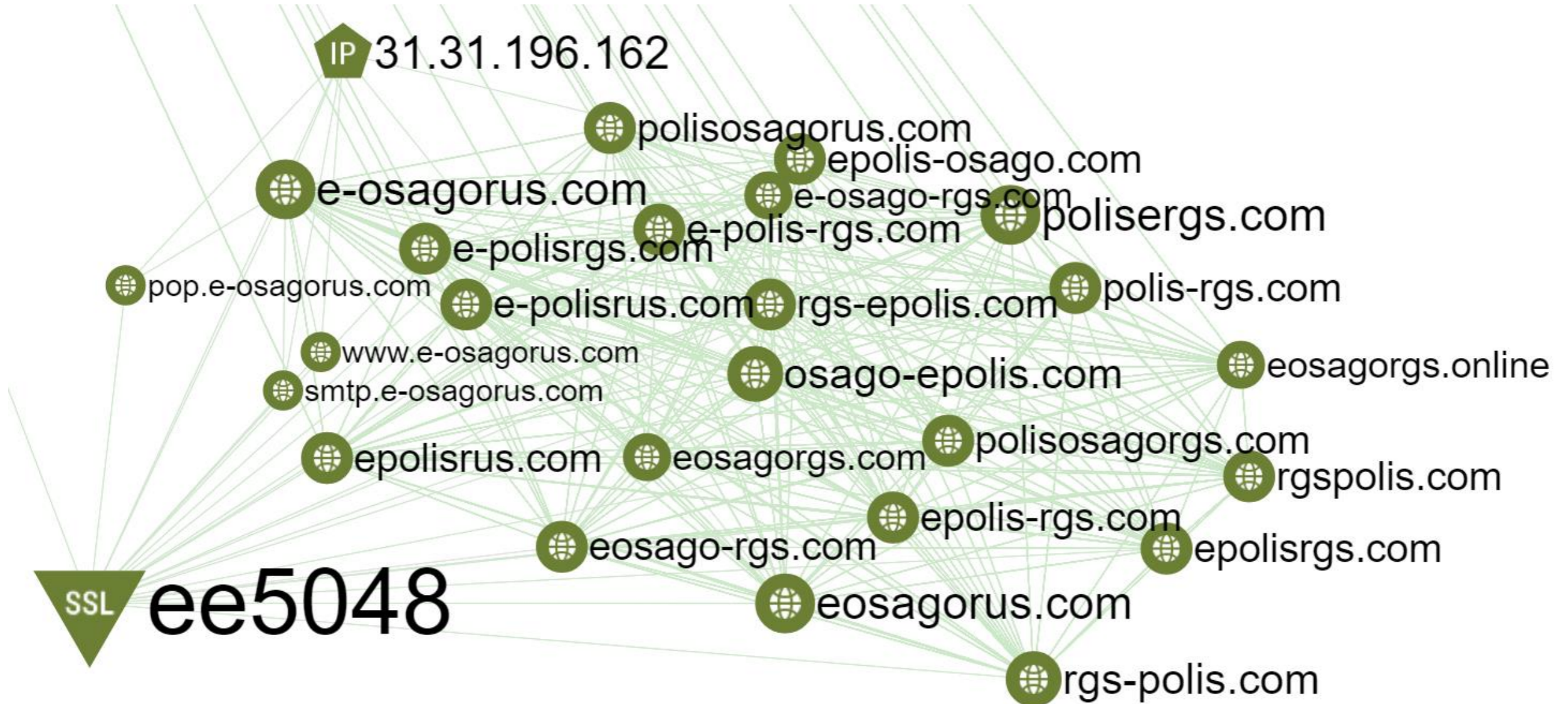


Domains ²⁵ IP addresses ¹ SSH fingerprints ⁰ SSL-certificates ¹ Files ⁰ Email ²³ Phone ³ Neighbours Communities

Domain name	Registrar	Reg date	Exp date	Email	Phone	Organization	Name
e-osagorus.com	1API GmbH	2017-06-10	2018-06-10	serjlazarev17@gmail.com	+7.9269481554	RosBroker	Sergei Lazarev
eosagorgs.com				serjlazarev17@gmail.com	+7.9269481554	RosBroker	Sergei Lazarev
eosagorus.com	1 API GmbH	2017-06-10	2018-06-10	legal@1api.net	+7.9269481554	RosBroker	Sergei Lazarev
epolis-rgs.com	1 API GMBH	2017-05-18	2018-05-18	serjlazarev17@gmail.com	+7.9269481554	RosBroker	Sergei Lazarev
epolis-osago.com	1 API GMBH	2017-06-06	2018-06-06	serjlazarev17@gmail.com	+7.9269481554	RosBroker	Sergei Lazarev
rgs-epolis.com	1API GmbH	2017-05-25	2018-05-25	serjlazarev17@gmail.com	+7.9269481554	RosBroker	Sergei Lazarev
polis-rgs.com	1 API GmbH	2017-05-24	2018-05-24	abuse@1api.net	+7.9269481554	RosBroker	Sergei Lazarev
eosagorgs.online	1API GmbH	2017-04-11	2018-04-11	serjlazarev17@gmail.com	+7.9269481554	RosBroker	Sergei Lazarev



Создание сети мошеннических сайтов одним злоумышленником





Создание однотипных сайтов разными заказчиками



rgs-epolice-osago.ru/calc.php

Подробнее о Е-ОСАГО

Расчет и оформление ОСАГО

РОСГОССТРАХ

Уважаемые клиенты! Внимательно и корректно заполняйте все поля для правильного расчета и оформления электронного полиса.

Расчет и покупка онлайн

1 Расчет

Регион собственника по паспорту
77, 97, 99, 177, 197, 199 Москва

ТРАНСПОРТНОЕ СРЕДСТВО

Легковые автомобили (ТС категории "B")

Мощность двигателя, л.с.

Срок страхования 12 месяцев

Начало действия полиса

Цель использования
Личная

Неограниченное количество водителей

ВОДИТЕЛЬ

Фамилия Имя Отчество

Дата рождения

rgs-epolice-osago.ru

rgs-services-osagos.ru/calc.php

Подробнее о Е-ОСАГО

Расчет и оформление ОСАГО

РОСГОССТРАХ

Уважаемые клиенты! Внимательно и корректно заполняйте все поля для правильного расчета и оформления электронного полиса.

Расчет и покупка онлайн

1 Расчет

Регион собственника по паспорту
77, 97, 99, 177, 197, 199 Москва

ТРАНСПОРТНОЕ СРЕДСТВО

Легковые автомобили (ТС категории "B")

Мощность двигателя, л.с.

Срок страхования 12 месяцев

Начало действия полиса

Цель использования
Личная

Неограниченное количество водителей

ВОДИТЕЛЬ

Фамилия Имя Отчество

Дата рождения

rgs-services-osagos.ru

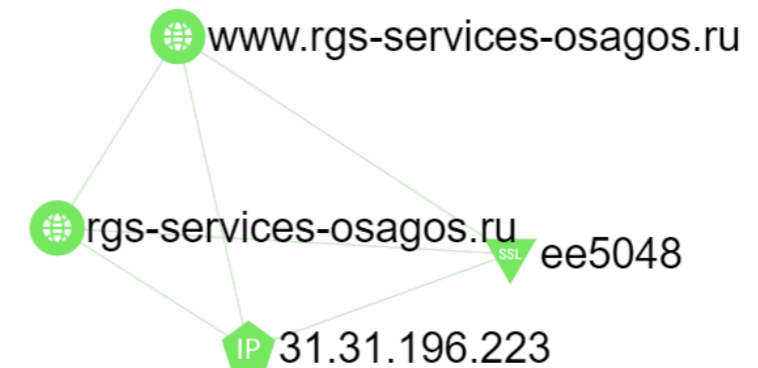


Создание однотипных сайтов разными заказчиками



Domains ² IP addresses ¹ SSH fingerprints ⁰ SSL-certificates ¹ Files ⁰ Email ⁰ Phone ⁰ Neighbours Communities

Domain name	Registrar	Reg date	Exp date	Email	Phone	Organization	Name
rgs-epolice-osago.ru	REGRU-RU	2017-12-04	2018-12-04				Private Person
www.rgs-epolice-osago.ru							

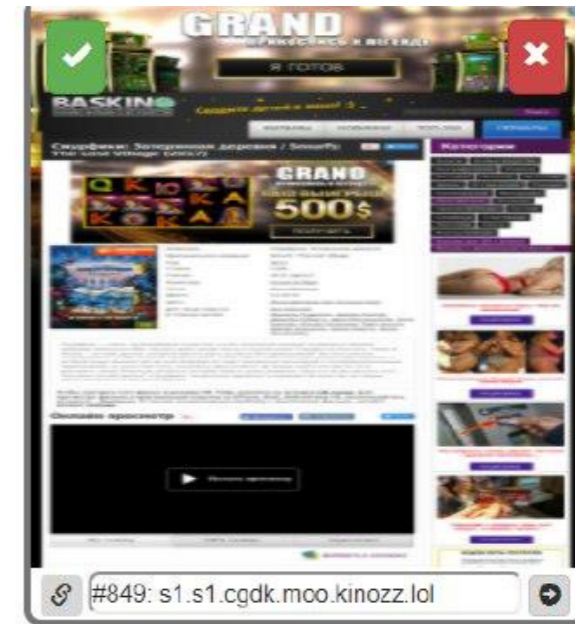
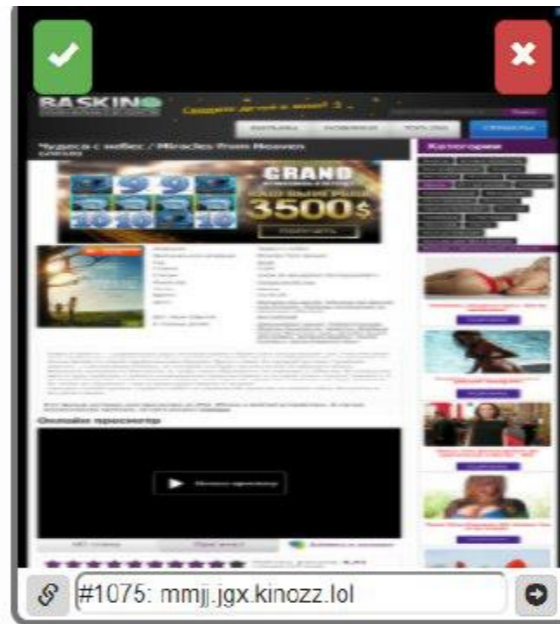


Domains ² IP addresses ¹ SSH fingerprints ⁰ SSL-certificates ¹ Files ⁰ Email ⁰ Phone ⁰ Neighbours

Domain name	Registrar	Reg date	Exp date	Email
rgs-services-osagos.ru	REGRU-RU	2017-12-07	2018-12-07	
www.rgs-services-osagos.ru				



Технологии распознавания визуальных образов





Незаконное использование товарного знака в сфере страхования

GROUP|IB

ESOSAGO-NN.RU

г. Н.Новгород, улица Родионова, 169А
ПН-ПТ 10:00 - 19:00 СБ 10:00 - 15:00

+7 (930) 283-73-88
Esosago-nn@yandex.ru

ГЛАВНАЯ ОСАГО КАСКО СТРАХОВАНИЕ НЕДВИЖИМОСТИ ДОСТАВКА ON-LINE ЗАЯВКА КОНТАКТЫ [ЗАКАЗАТЬ ЗВОНОК](#)

СТРАХОВАНИЕ НЕДВИЖИМОСТИ ОТ ЛУЧШИХ СТРАХОВЫХ КОМПАНИЙ С ДОСТАВКОЙ НА ДОМ



- ✓ Доставка страховки за 2 часа
- ✓ Скидки до постоянным клиентам
- ✓ Лучшие страховые компании России

ИНГОССТРАХ
Ingostrakh

АЛЬФА
СТРАХОВАНИЕ



[ЗАКАЗАТЬ СЕЙЧАС](#)

Доставка **БЕСПЛАТНО** при страховке 3 объектов недвижимости
(доставка в пределах Н.Новгорода – 300 р, выезд в Нижегородской области не далее 30 км от НН – по договоренности)

ESOSAGO-NN.RU

г. Н.Новгород, улица Родионова, 169А
ПН-ПТ 10:00 - 19:00 СБ 10:00 - 15:00

+7 (930) 283-73-88
Esosago-nn@yandex.ru

ГЛАВНАЯ ОСАГО КАСКО СТРАХОВАНИЕ НЕДВИЖИМОСТИ ДОСТАВКА ON-LINE ЗАЯВКА КОНТАКТЫ [ЗАКАЗАТЬ ЗВОНОК](#)

СТРАХОВАНИЕ НЕДВИЖИМОСТИ ОТ ЛУЧШИХ СТРАХОВЫХ КОМПАНИЙ С ДОСТАВКОЙ НА ДОМ



- ✓ Доставка страховки за 2 часа
- ✓ Скидки до постоянным клиентам
- ✓ Лучшие страховые компании России

ИНГОССТРАХ
Ingostrakh

АЛЬФА
СТРАХОВАНИЕ





[ЗАКАЗАТЬ СЕЙЧАС](#)

Доставка **БЕСПЛАТНО** при страховке 3 объектов недвижимости
(доставка в пределах Н.Новгорода – 300 р, выезд в Нижегородской области не далее 30 км от НН – по договоренности)




Мошенничество в сфере страхования





СТРАХОВКА
ONLINE

info@strahovka-online.com
[+8 \(800\) 100 83 81 \(Бесплатно\)](tel:+8(800)1008381)

[strahovka-online](#)






[Заказать услугу](#)

[Главная](#) / [Страхование недвижимого имущества](#)


КАК ЗАСТРАХОВАТЬ СВОЮ НЕДВИЖИМОСТЬ НАИБОЛЕЕ ПРОСТЫМ И ВЫГОДНЫМ СПОСОБОМ?


Каковы бы ни были цели страхования, итог один: делается это для уменьшения финансовых рисков при порче или потере имущества. Чтобы минимизировать еще и временные потери на поиск страховой компании, изучение условий, оформление документации, наша компания предлагает воспользоваться онлайн-сервисом.


НАШИ ПРЕИМУЩЕСТВА

- 
Предоставление полной и доступной к пониманию информации
 Большинство людей не любят разбираться в хитросплетении юридических, научных терминов и выдвигают своим клиентам. На нашем сайте Страховка онлайн вся информация подана просто и понятно, из чего составляется стоимость страхового полиса, в каких случаях страховка действует.
- 
Онлайн-калькулятор
 На сайте Вы можете самостоятельно рассчитать стоимость страхования своей недвижимости с дополнительными опциями. Преимущество онлайн-калькулятора – Вы можете провести расчеты в любое удобное время, на поездку, консультации.
- 
Онлайн-оплата
 Чтобы оплатить полис, не нужно даже выезжать в банк. Наша компания принимает оплату в любое удобное время дня или даже ночи.
- 
Получение полиса на e-майл
 Еще никогда получение страховки не было такой легкой и простой процедурой. Вам не нужно идти в офис, чтобы получить полис.

Выберите способ оплаты:

 **С банковской карты**
 Visa, MasterCard, Maestro

 **С баланса мобильного**
 привязанного к кошельку


 **Наличными**
 в Сбербанке, Евросети и тд..

Реквизиты для оплаты на Яндекс кассу:


Счет: 1411_151067908214115757

Сумма к оплате: 3378.95 RUB

Фамилия

 Anastasiya


Почта

 ligof@yandex.ru

Имя

 Klimova

Телефон

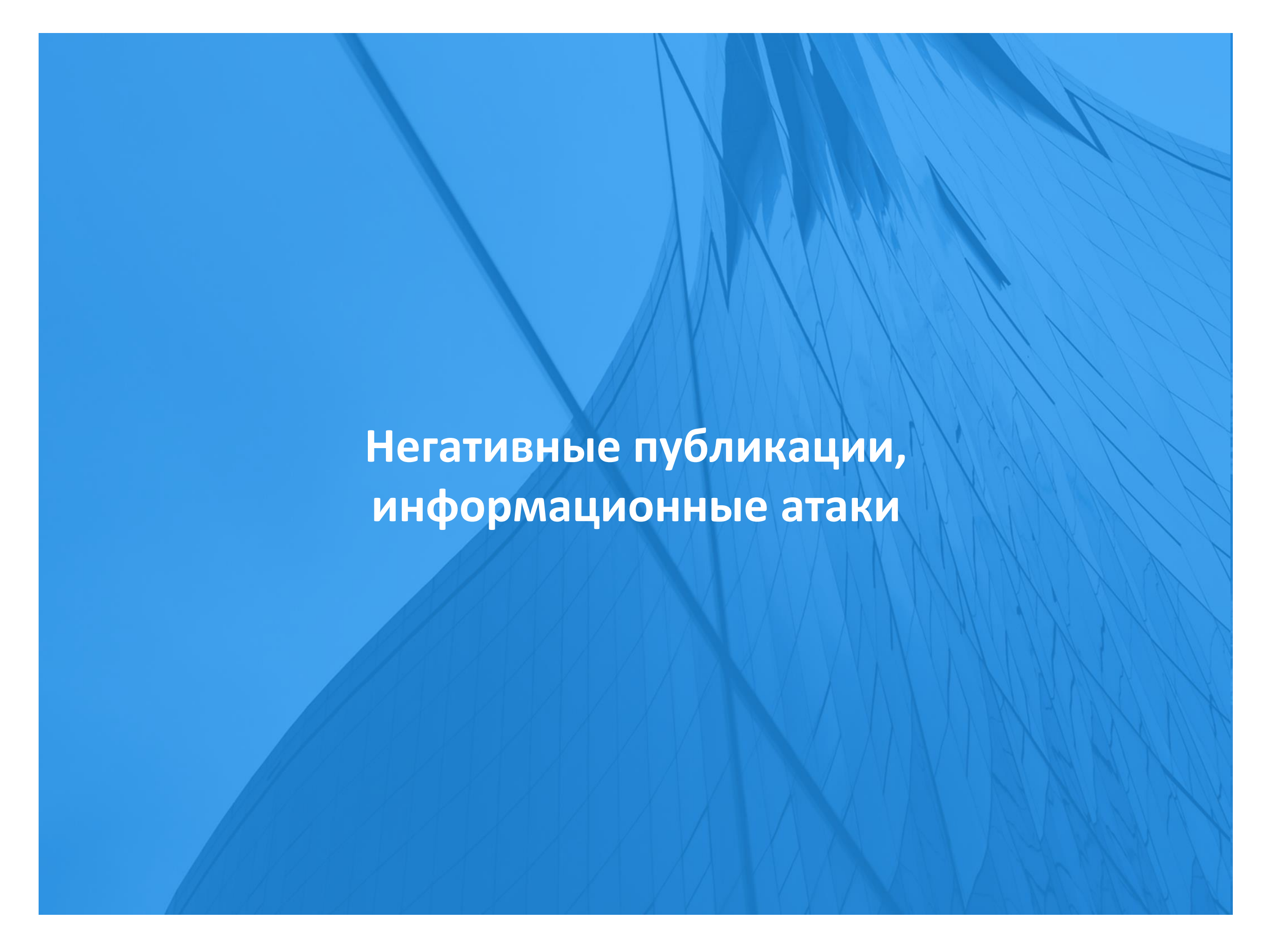
 89683551407

[Оплатить](#)



Анализируйте мошеннические сайты: один сайт может вывести на десятки других связанных с ним сайтов

1. Превентивно регистрируйте схожие доменные имена
2. Постоянно мониторьте доменные имена, поисковую выдачу, базу фишинговых ресурсов
3. Отслеживайте способы их продвижения: контекстную рекламу, посты в соцсетях и мессенджерах
4. Следите за использованием вашего товарного знака на сторонних ресурсах
5. Выявляйте аналогичные мошеннические сайты при помощи анализа связей и аффилированности сайтов
6. Блокируйте мошеннические ресурсы: обращайтесь к компаниям со специальной компетенцией по блокировке сайтов

The background is a solid blue color with a subtle, light-colored grid pattern. A large, dark blue 'X' shape is overlaid on the grid, extending from the corners towards the center. The text is centered in the middle of the 'X' and the grid.

Негативные публикации, информационные атаки



Почему необходимо следить за информационным полем бренда в сети

|GROUP|IB|

Пользователи ушли в интернет

85 млн пользователей в России пользуются интернетом и ежемесячно публикуют 500 млн сообщений в соцсетях

Атаки происходят быстро

на раскрытие информационной атаки с охватом несколько миллионов пользователей злоумышленникам достаточно 2-4 дней

Атаки приводят к большим потерям

1,3 трлн рублей лишился Сбербанк за одну неделю в 2014 году в результате информационной атаки.

Негативные публикации, информационные атаки

Кейс производителя продуктов питания



Кейс производителя продуктов питания

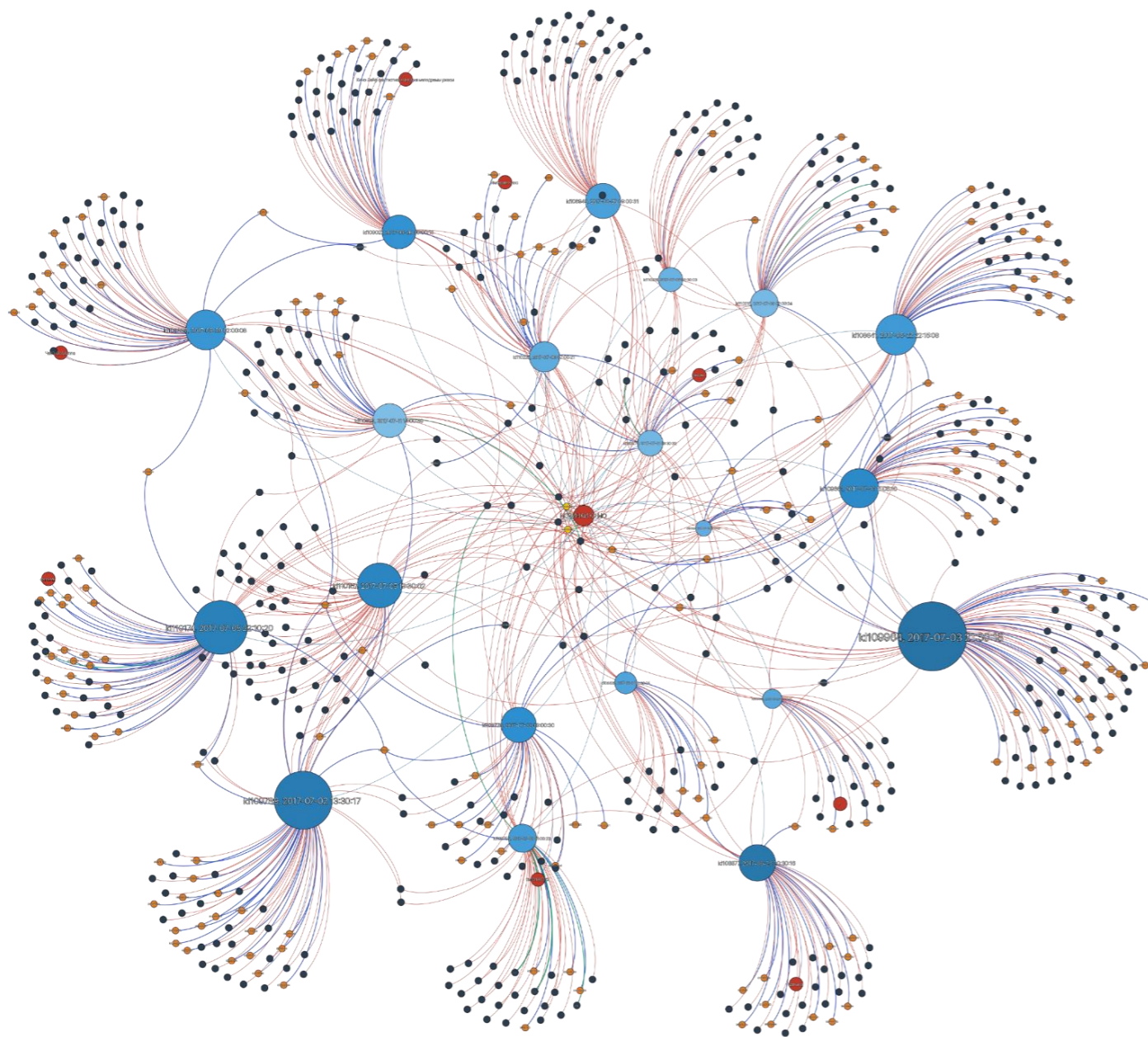


Летом 2017 года в соцсетях о продуктах известной компании-производителя начали распространяться отзывы об их негативном влиянии на самочувствие и здоровье в целом.

Это информационная атака или реальные отзывы?



Технологии выявления аффилированности групп в соцсетях



Вершины:

Синий – пост

Красный – группа

Оранжевый – «репостящий»
пользователь

Связи:

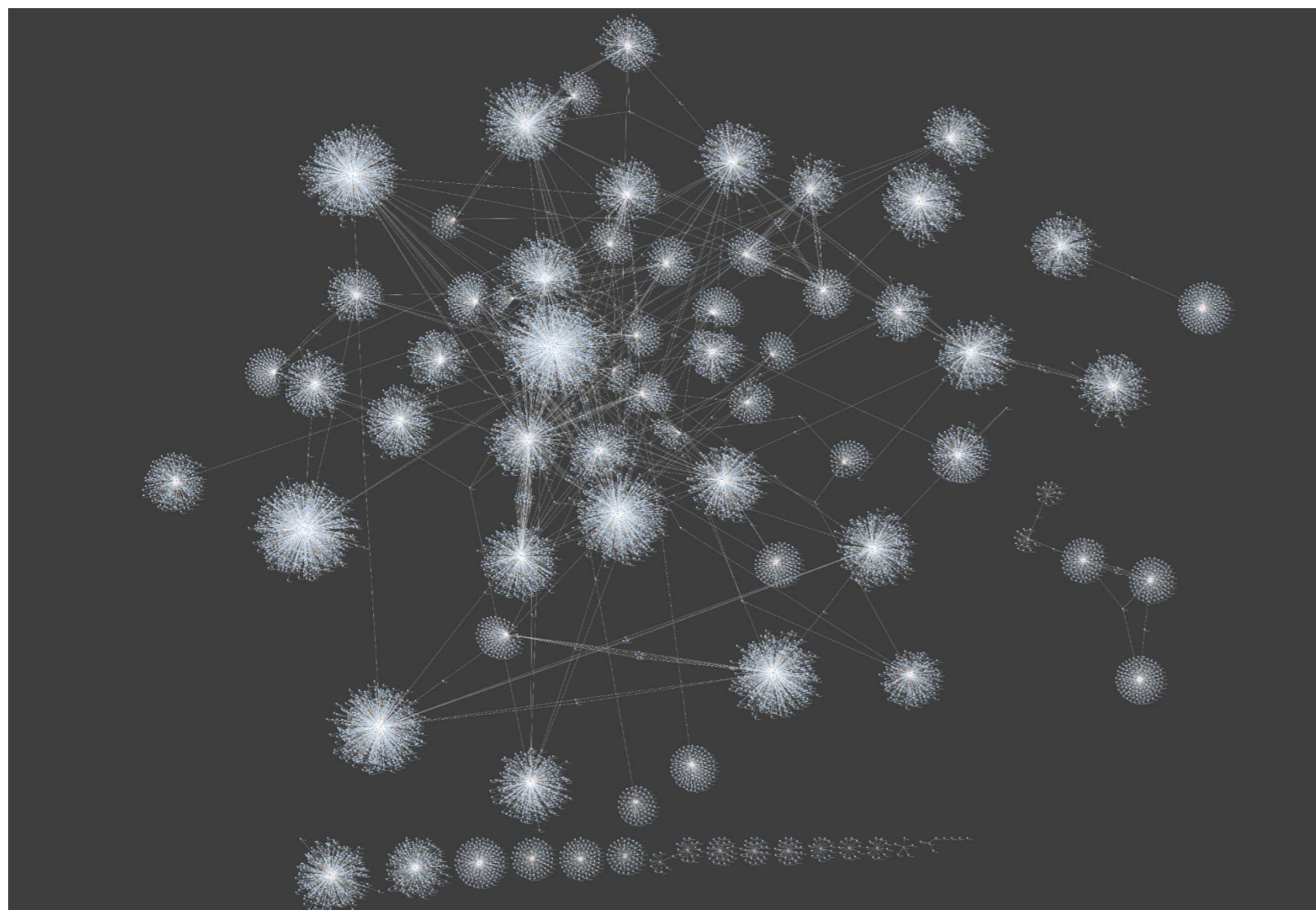
● Синий – репост

● Красный – лайк

● Зеленый – комментарий



Кейс производителя продуктов питания



15 410

человек

15 687

связей

Результаты автоматического анализа связей между постами:

- Группы людей очень хорошо связаны друг с другом
- Есть небольшое количество вбросов

Вывод:

Информация распространялась по «сарафанке»



Выявляйте информационные атаки на этапе их зарождения

1. Отслеживайте упоминания своего бренда в постах в соцсетях
2. Анализируйте связи между ними – это возможно при помощи технологий Big Data
3. Оперативно принимайте контрмеры



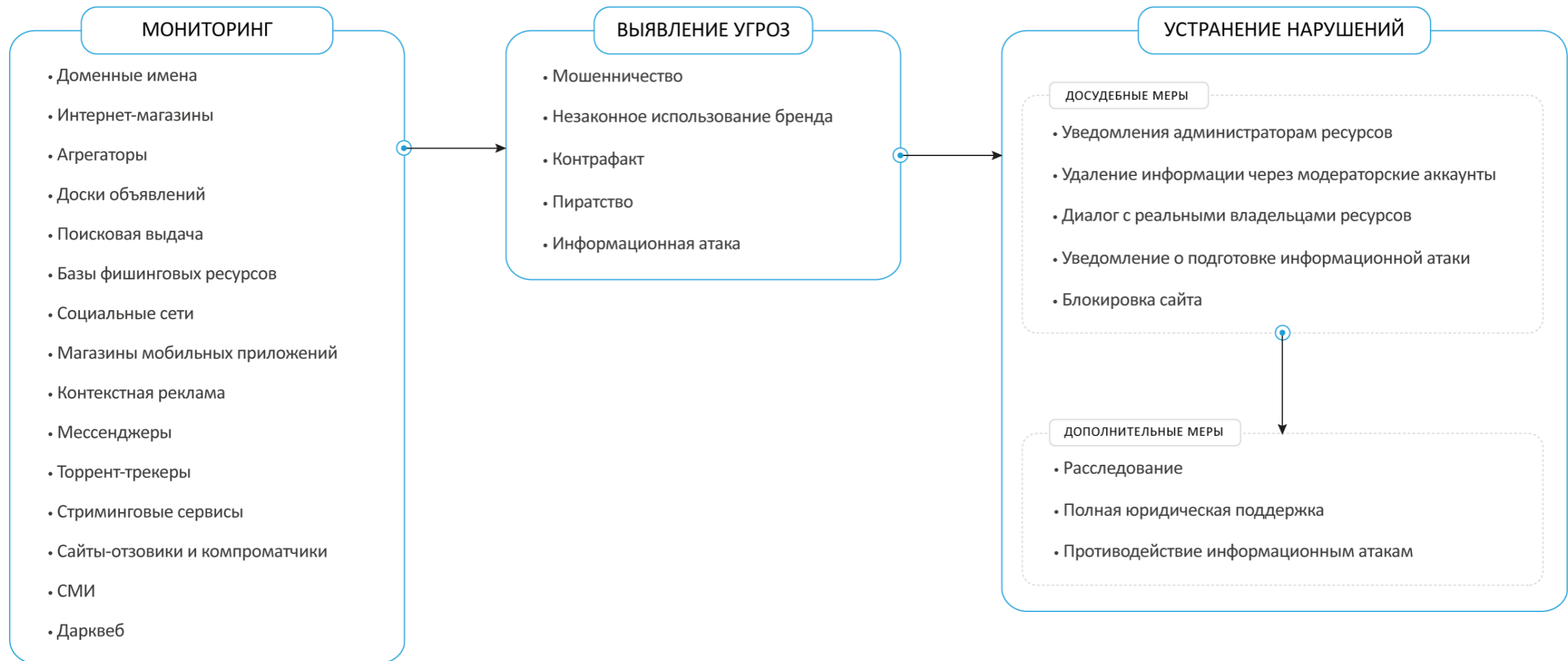
Group-IB Brand Protection



Group-IB Brand Protection



Технологический сервис по выявлению и устранению угроз, направленных против вашего бренда в интернете.





Секреты эффективного решения



Передовые технологии кибербезопасности

Машинное обучение

Система самостоятельно квалифицирует нарушения на основе предыдущего опыта.

Технология анализа больших данных

Позволяет автоматически выявлять связи между сайтами и между группами в соцсетях.

Технологии киберразведки

Позволяют устанавливать прямой контакт с нарушителями.

Команда профессионалов

Собственный центр оперативного реагирования – CERT-GIB

Компетенции по блокировке мошеннических ресурсов в доменных зонах .RU, .РФ и .SU и реагирование за их пределами.

Опытные криминалисты и эксперты отдела расследований

Специалисты с многолетним опытом расследования случаев распространения контрафакта и интернет-мошенничества.

Репутация

Среди киберпреступников

Получив уведомление, нарушители предпочитают не игнорировать требования компании, добившейся приговоров для десятков киберпреступников.

Среди регистраторов и хостинг-провайдеров

Репутация Group-IB позволяет нам быстрее находить понимание по всему миру и добиваться содействия в устранении нарушения в самые короткие сроки.

3 млн ресурсов

автоматически отслеживаются круглосуточно

10 тысяч

нарушений устраняется ежедневно

85% нарушений

устраняются в досудебном порядке



Андрей Бусаргин

busargin@group-ib.com

+7 915 350 76 42

Предотвращаем и расследуем
киберпреступления с 2003 года.

www.group-ib.ru

info@group-ib.ru

twitter.com/groupib

t.me/group_ib

group-ib.ru/blog

+7 495 984 33 64

facebook.com/group-ib

instagram.com/group_ib