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

Андрей Бусаргин
Директор направления Brand Protection

О Group-IB

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

Официальный партнёр EUROPOL и INTERPOL

Рекомендована Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)

Одна из 7 самых влиятельных компаний в области кибербезо-пасности по версии Business Insider

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

Онлайн-угрозы для страховых компаний

Угрозы	Схемы
Интернет-мошенничество, неправомерное использование бренда	• Мошеннические сайты, сайты-клоны, фишинг • Ложное партнерство • Неправомерная реклама • Поддельные аккаунты и группы в соцсетях
Информационные атаки	• Направленные бот-атаки против бренда • Распространение негатива о бренде и руководстве

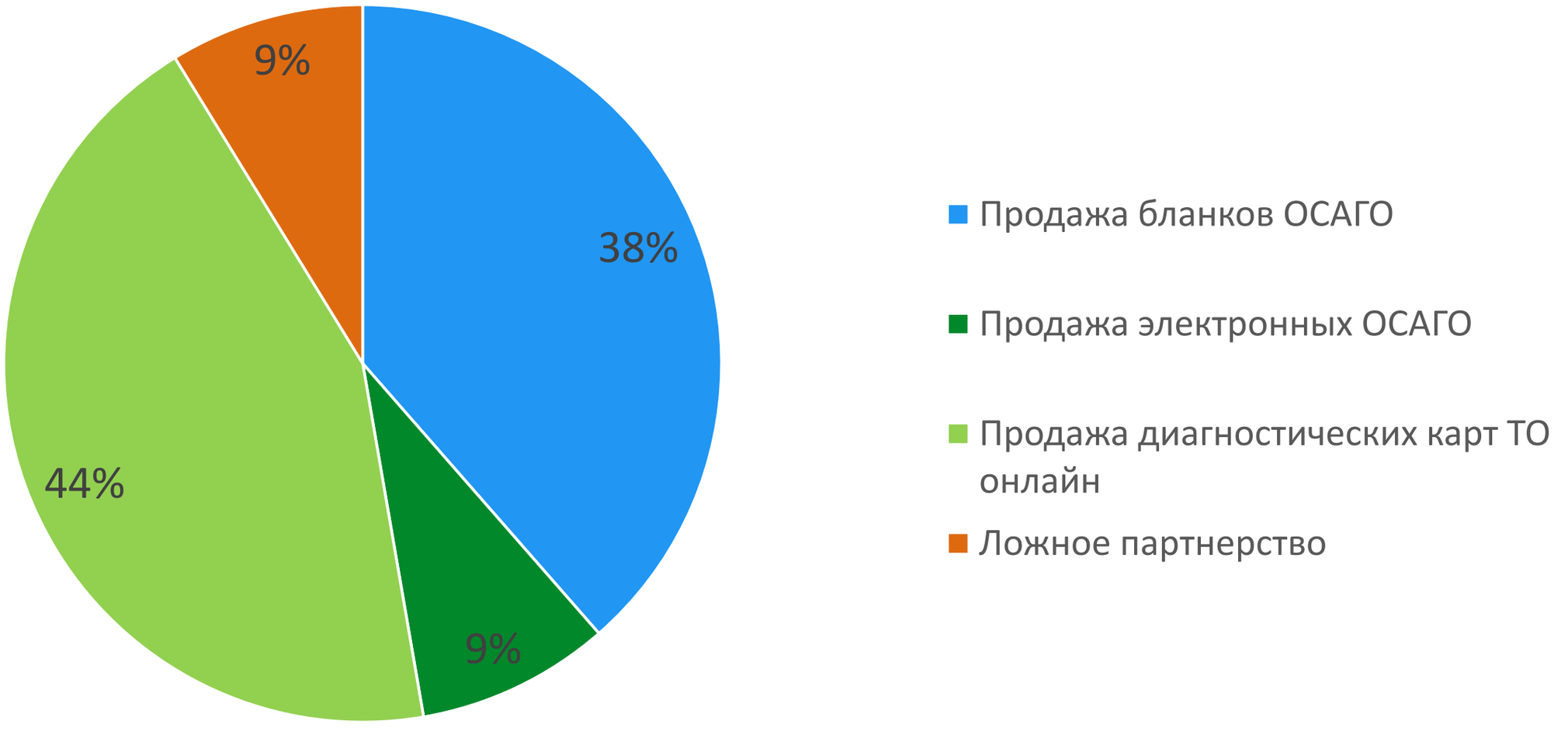
Интернет-мошенничество в России

100 млрд
рублей
ежегодный ущерб компаний в России от неправомерного использования их бренда

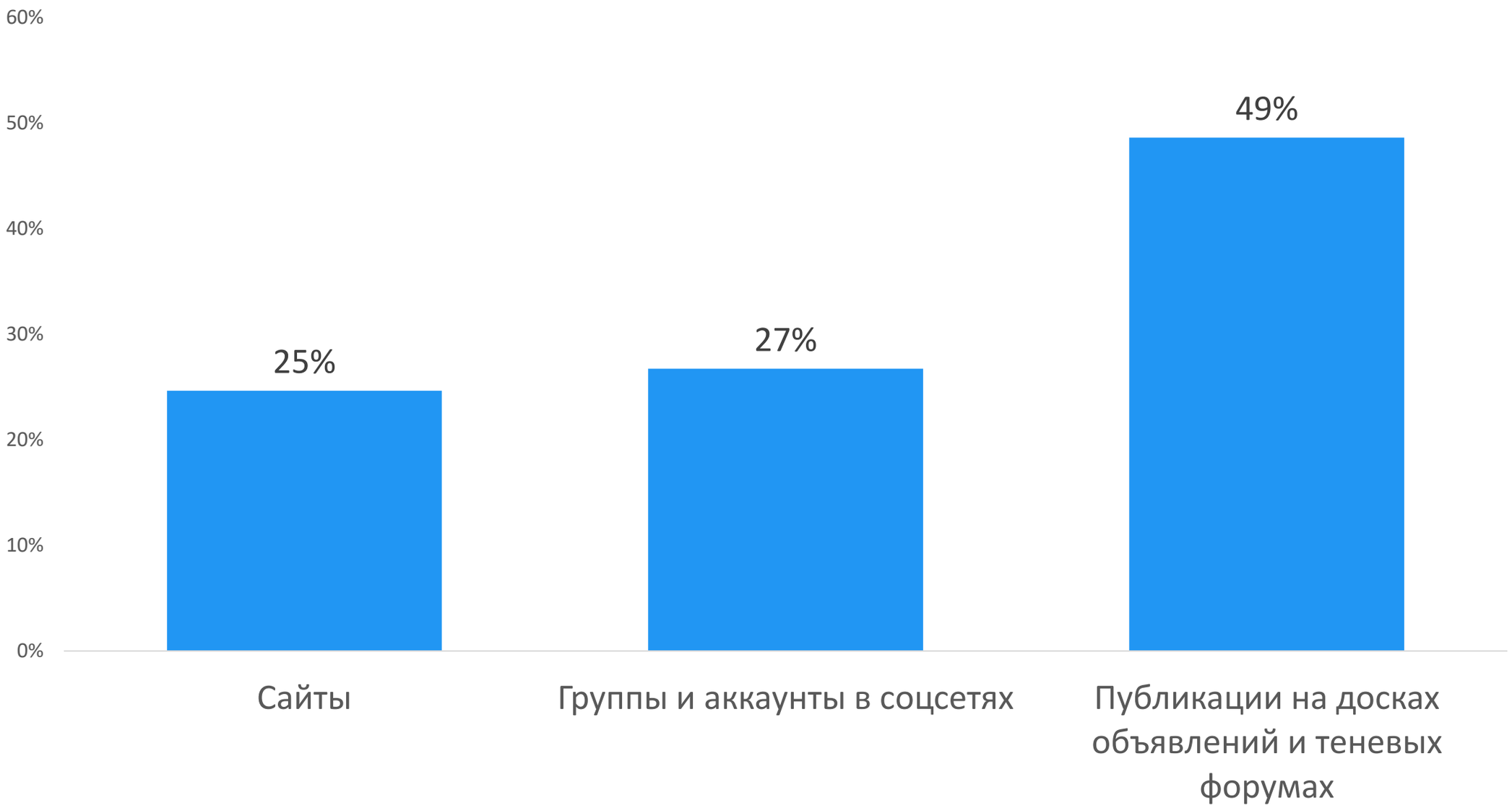
25 тысяч
сайтов
ежедневно создают мошенники в мире

750 млн
пользователей
в месяц попадают минимум на один мошеннический сайт

Нарушения в сфере автострахования в 2017 году

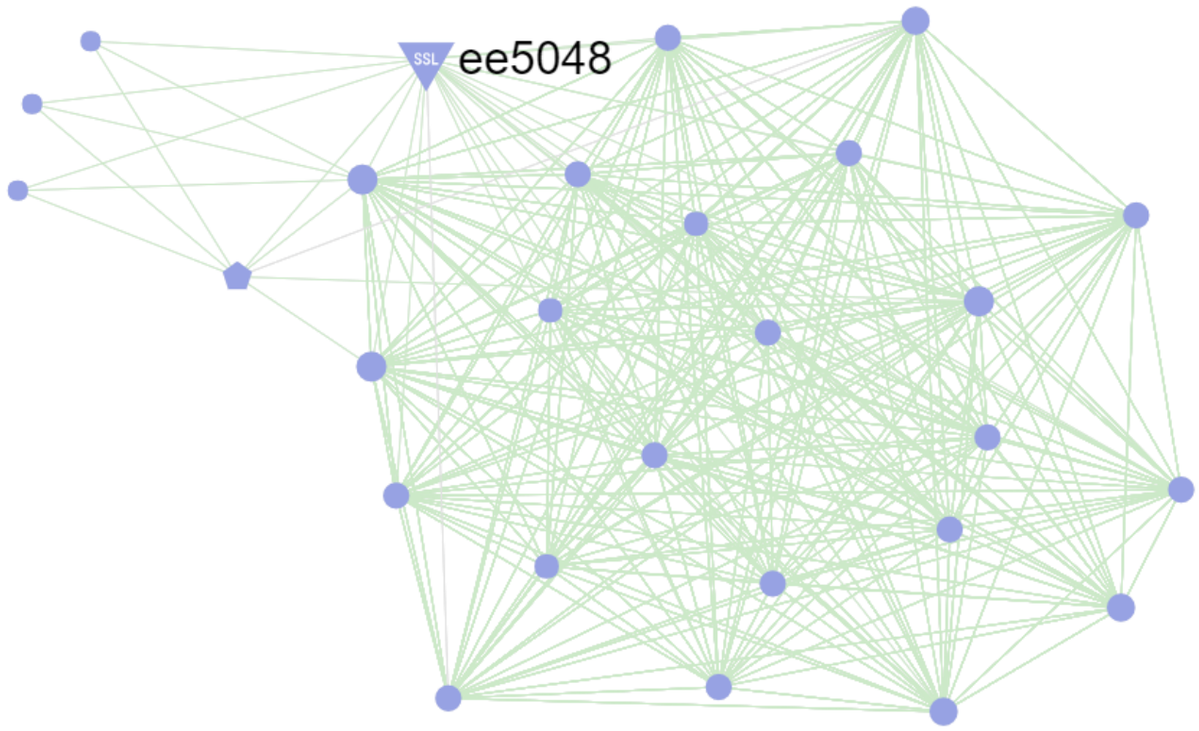


Онлайн-угрозы для страховых компаний



Как действуют онлайн-мошенники

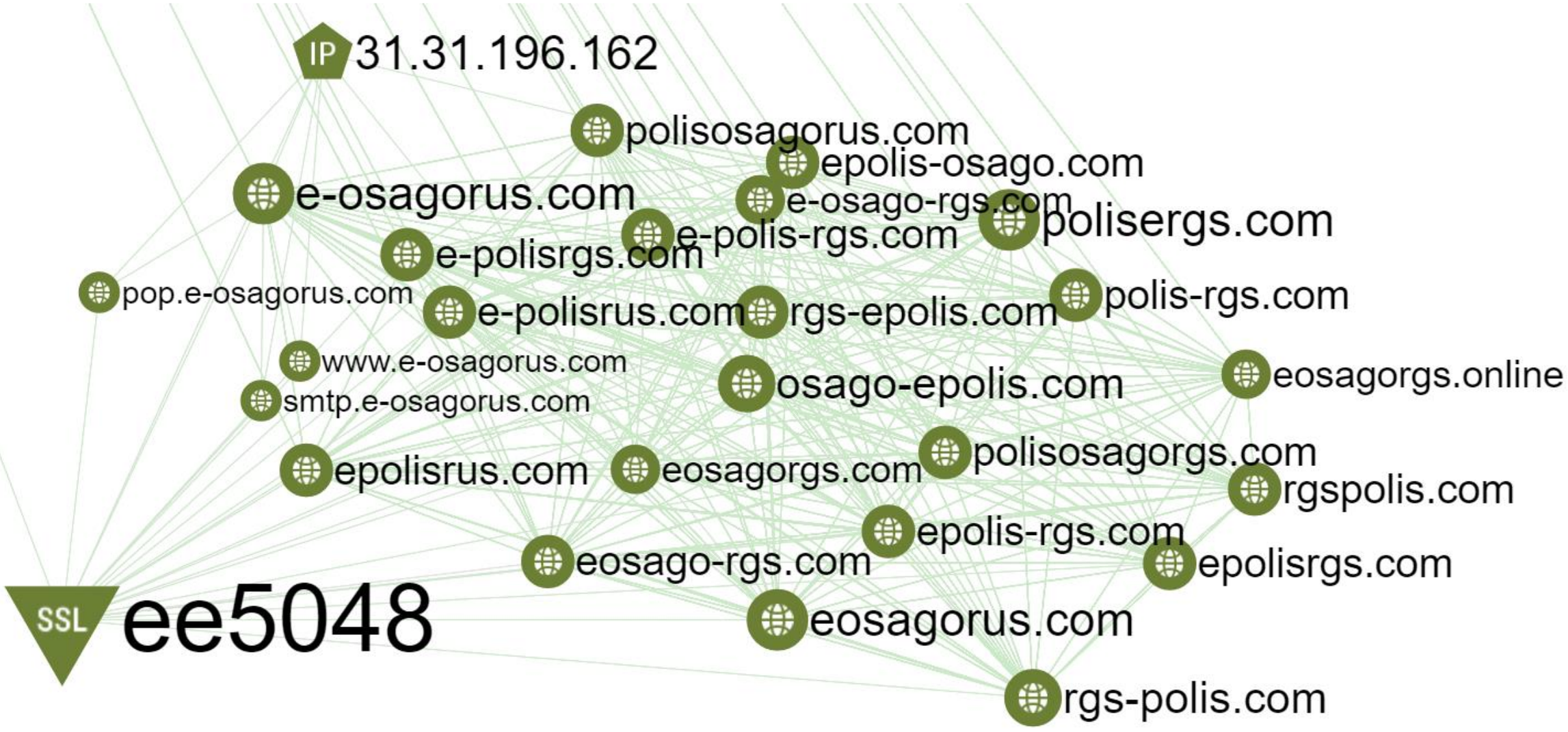
Создание сети мошеннических сайтов одним злоумышленником



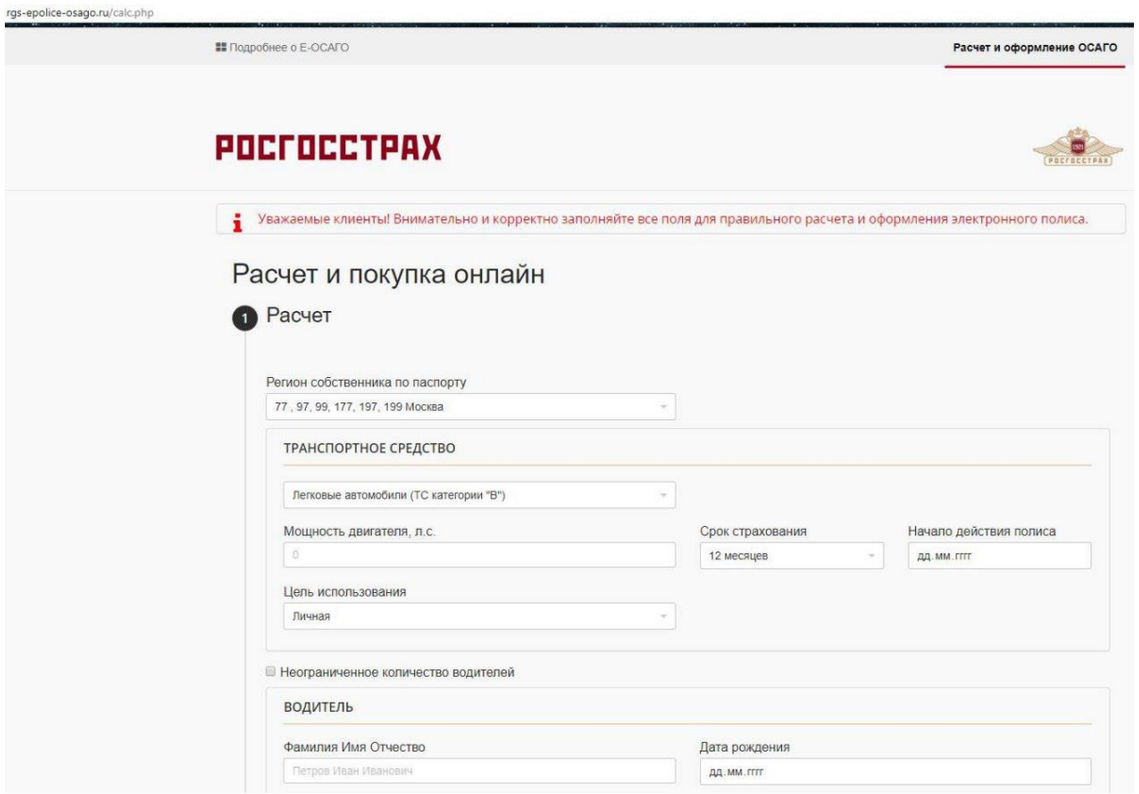
Domains 25 | IP addresses 1 | SSH fingerprints 0 | SSL-certificates 1 | Files 0 | Email 23 | Phone 3 | Neighbours | Communities

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

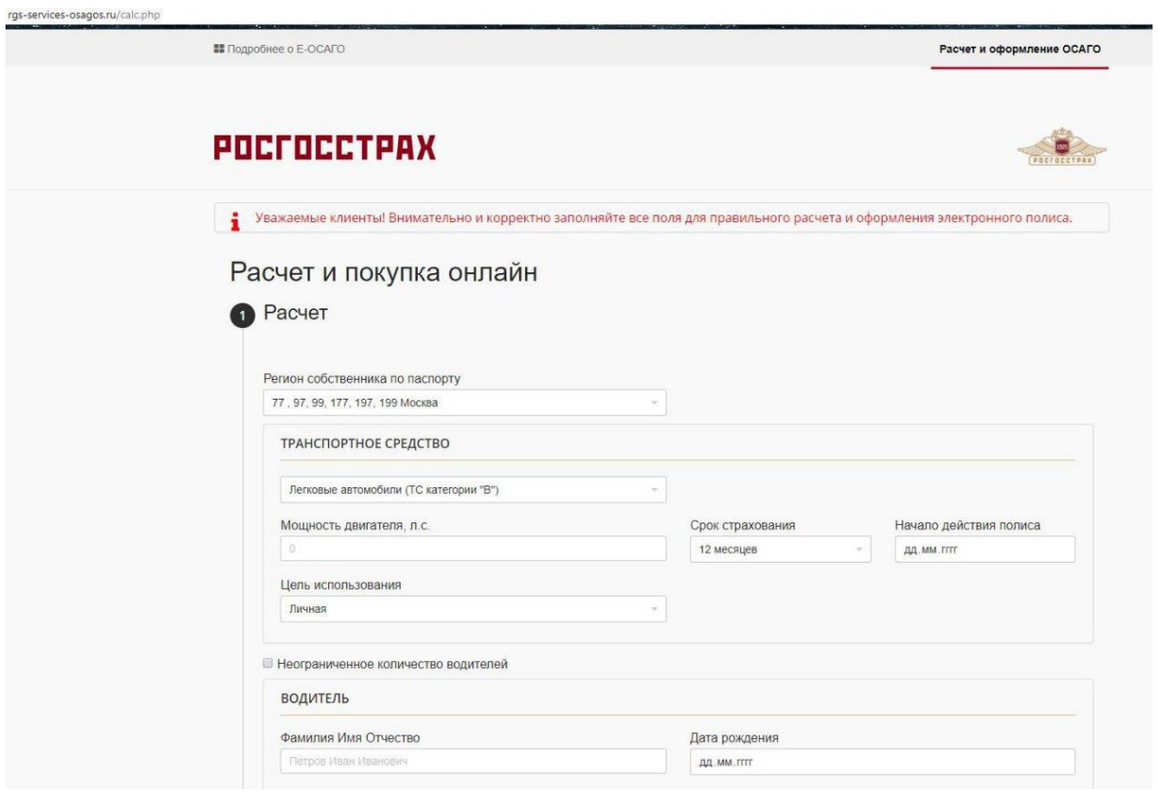
Создание сети мошеннических сайтов одним злоумышленником



Создание однотипных сайтов разными заказчиками



rgs-epolice-osago.ru



rgs-services-osagos.ru

Создание однотипных сайтов разными заказчиками

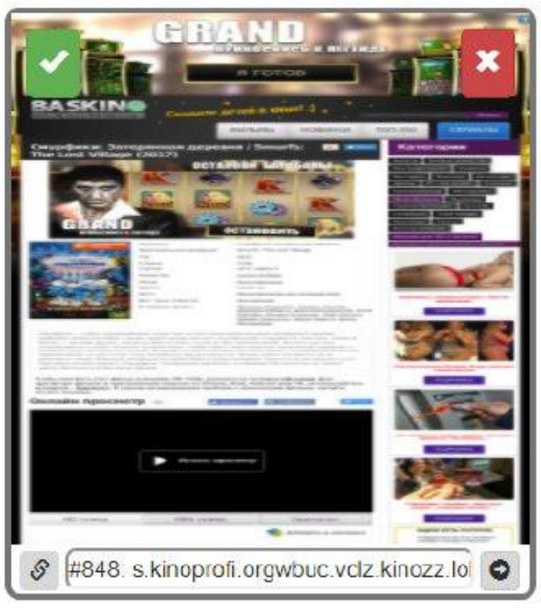
Domains 2 | IP addresses 1 | SSH fingerprints 0 | SSL-certificates 1 | Files 0 | Email 0 | Phone 0 | Neighbours | Communities

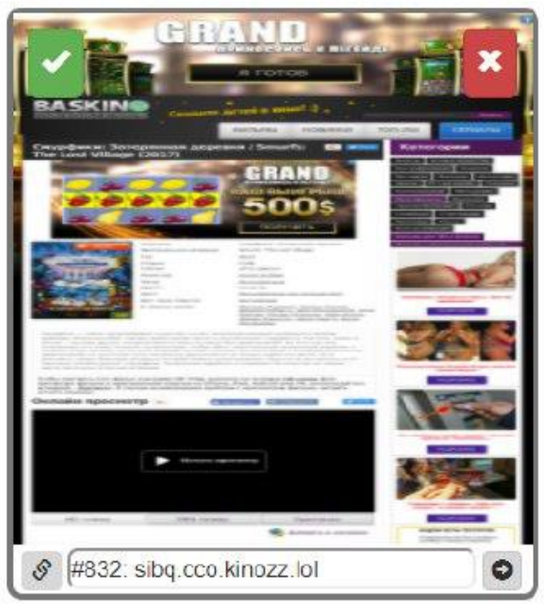
Domain name	Registrar	Reg date	Exp date	Email	Phone	Organization	Name
rgs-epolice-osago.ru	REGRU-RU	2017-12-04	2018-12-04				Private Person
www.rgs-epolice-osago.ru							

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

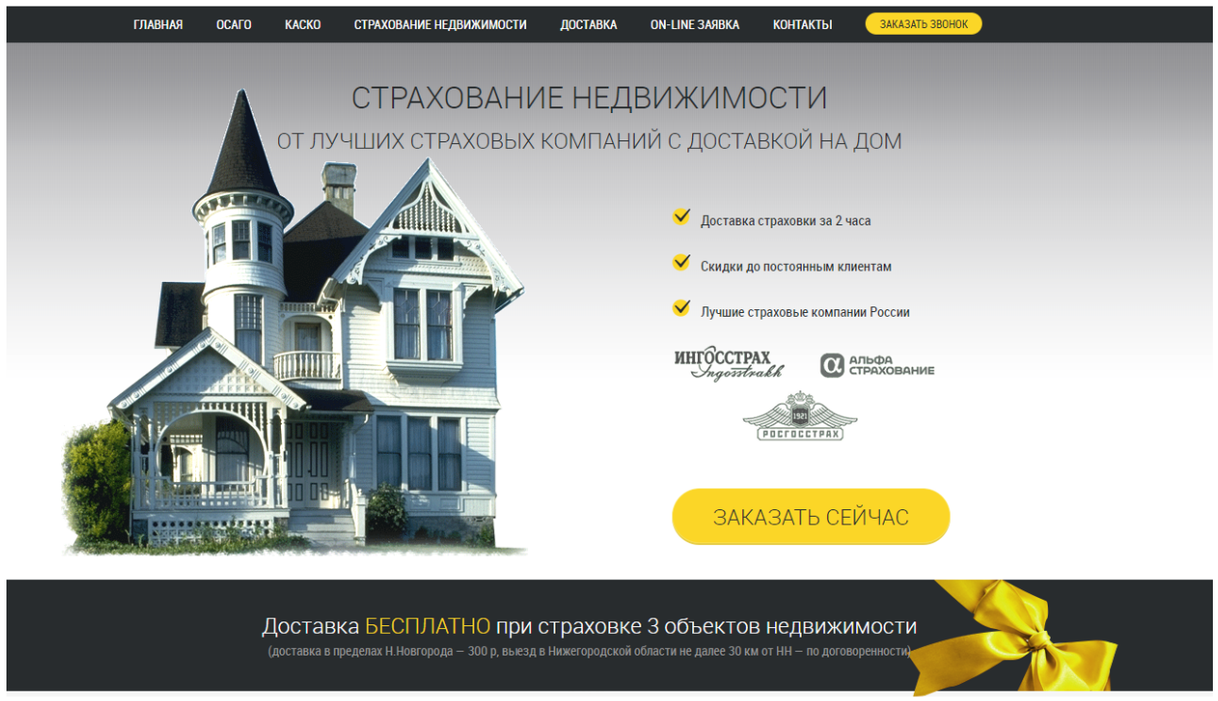
Domain name	Registrar	Reg date	Exp date	Email
rgs-services-osagos.ru	REGRU-RU	2017-12-07	2018-12-07	
www.rgs-services-osagos.ru				

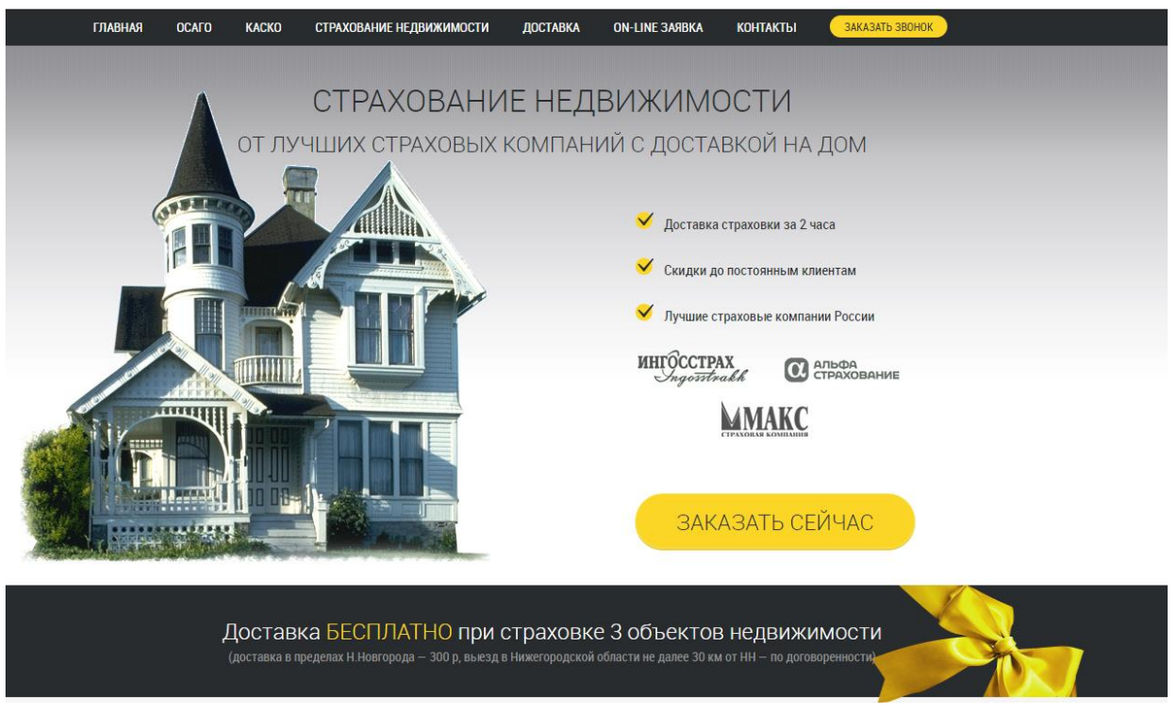
Технологии распознавания визуальных образов



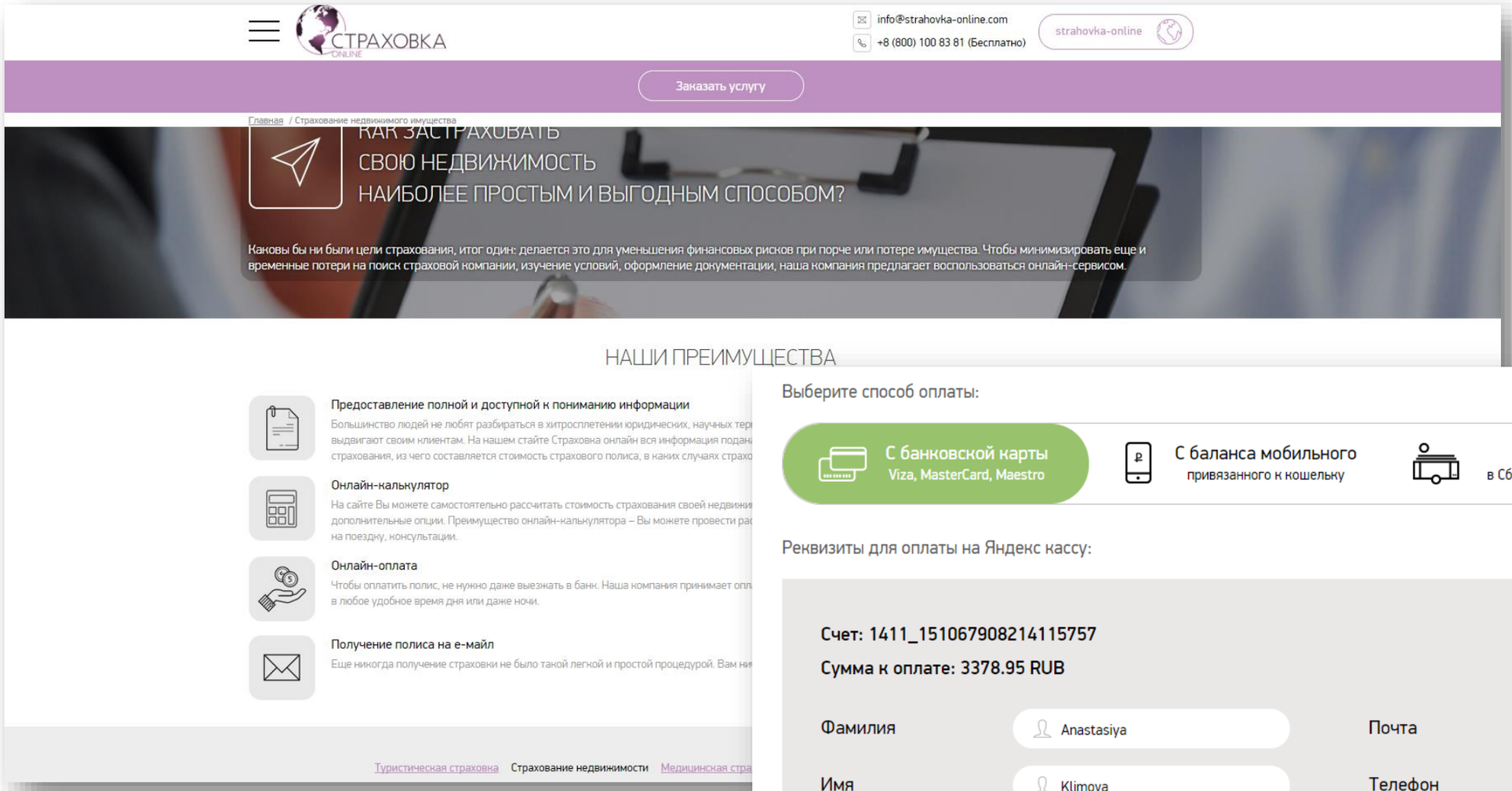


Незаконное использование товарного знака в сфере страхования





Мошенничество в сфере страхования



Рекомендации по борьбе с мошенниками

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

Негативные публикации, информационные атаки

Почему необходимо следить за информационным полем бренда в сети

Пользователи ушли в интернет

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

Атаки происходят быстро

на раскрутку 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

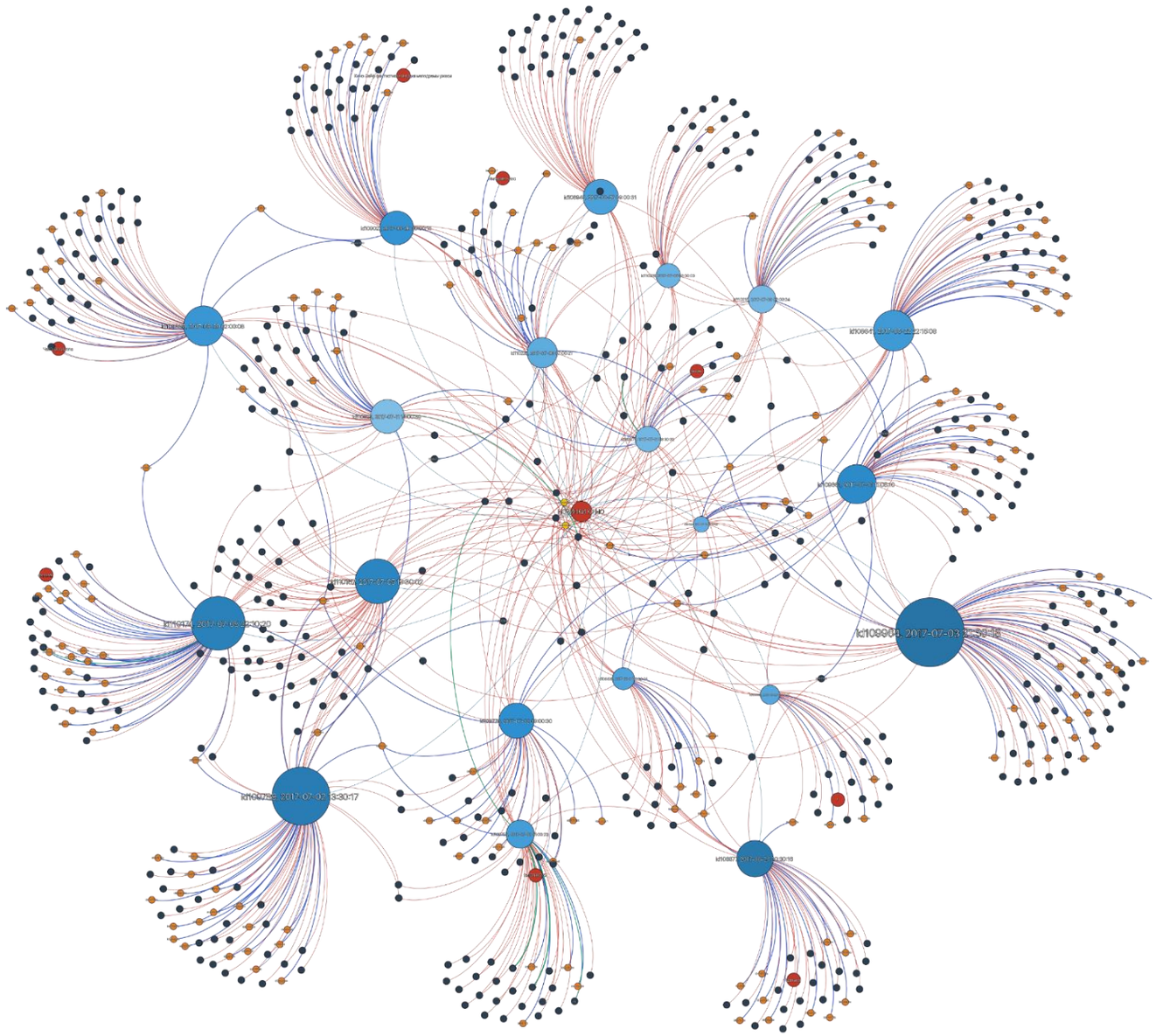
Кейс производителя продуктов питания

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

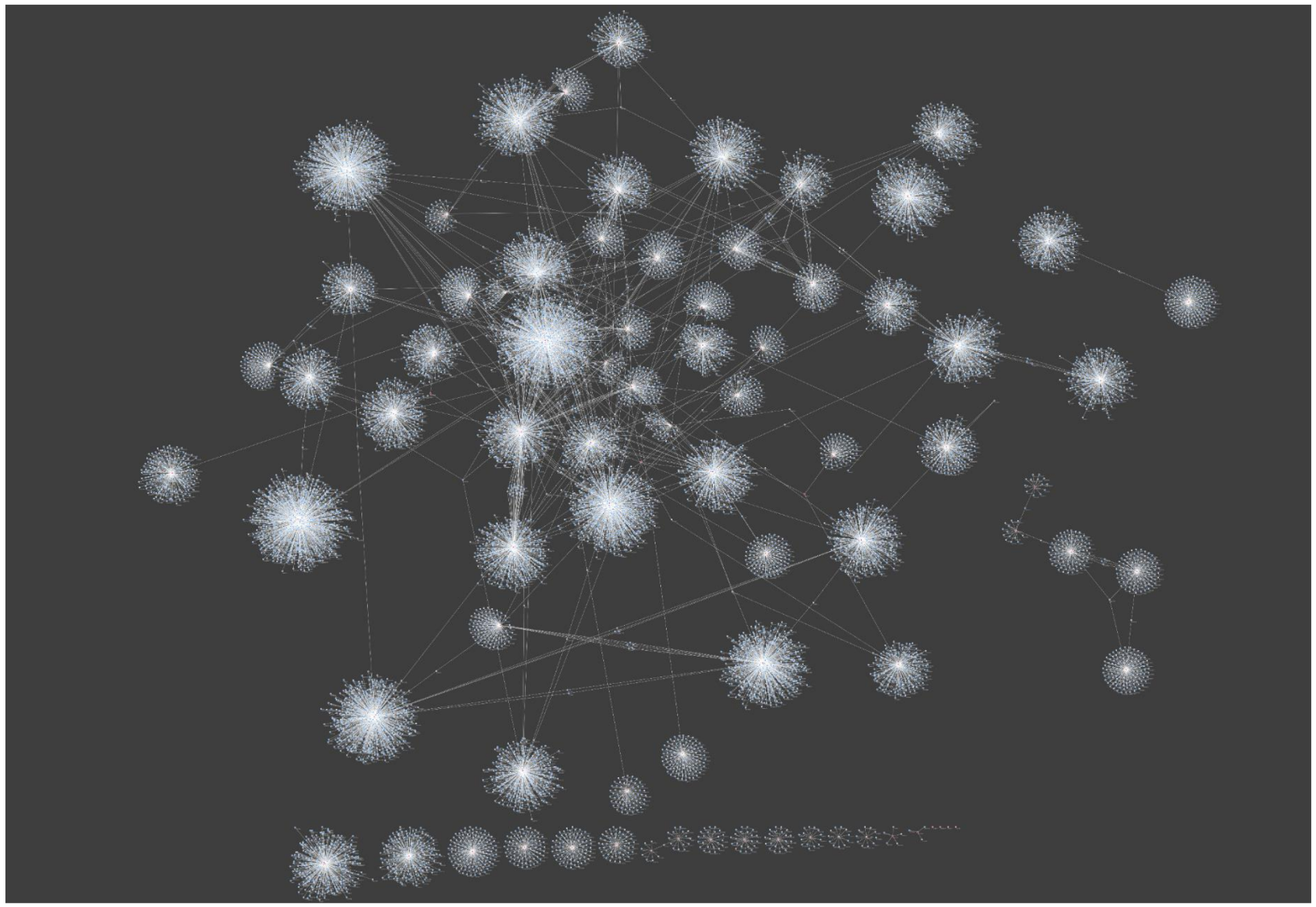
Красный – группа

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»

Рекомендации

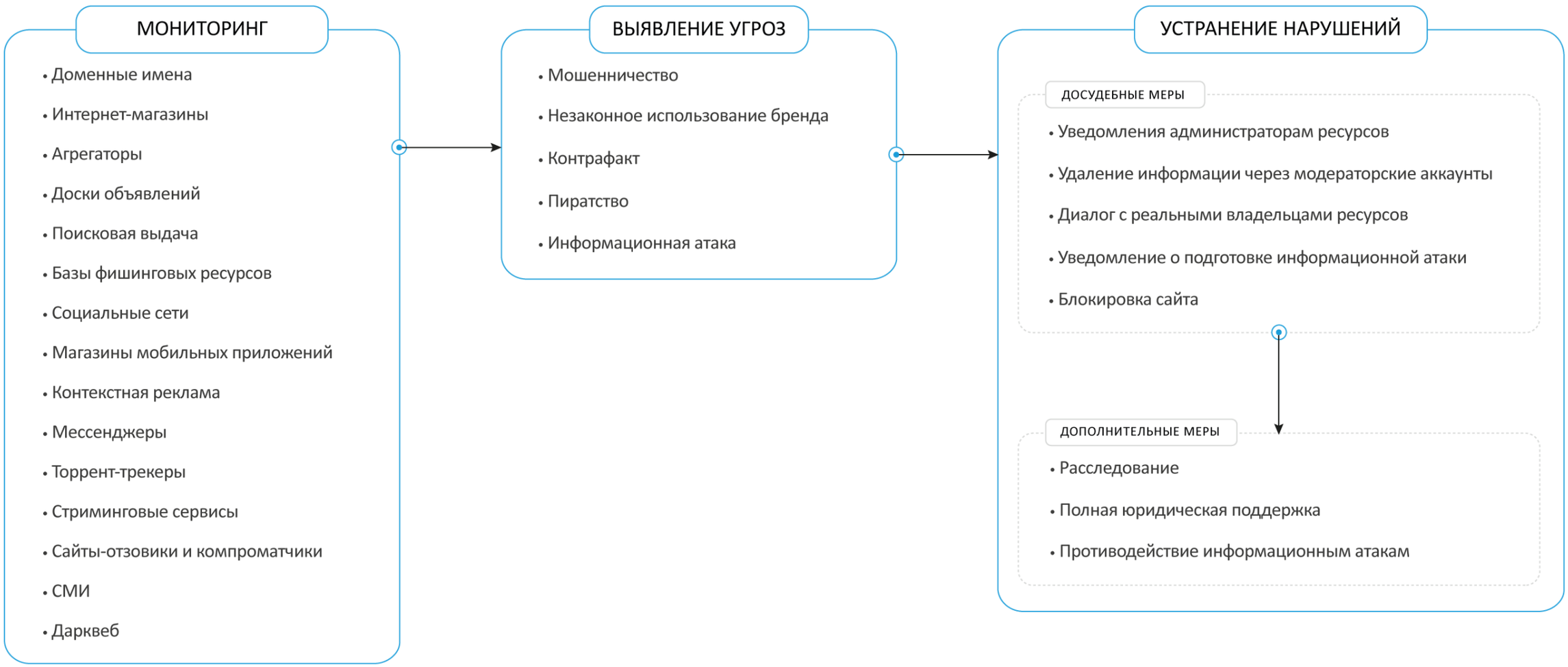
Выявляйте информационные атаки на этапе их зарождения

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.

3 млн ресурсов

автоматически отслеживаются круглосуточно

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.

10 тысяч

нарушений устраняется ежедневно

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.

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