

ОТРАСЛЕВАЯ ПЛАТФОРМА

СИСТЕМЫ БЕЗОПАСНОСТИ

#1 В РОССИИ

CONTENT SYNDICATION – ЛИДОГЕНЕРАЦИЯ И ПРОДВИЖЕНИЕ КОМПАНИИ ЧЕРЕЗ КОНТЕНТ

Многолетняя экспертиза журнала "Системы безопасности", воплощенная в цифровых сервисах и эффективном комьюнити профессионалов

Комплексные услуги www.secuteck.ru гарантируют расширение списков потенциальных клиентов ежемесячно или ежеквартально – вы получите верифицированную аудиторию с подтвержденными интересами в вашей теме и к вашим технологиям: руководители и специалисты, которые находятся в поиске решений своих задач в данный конкретный момент времени.

Как это работает

2

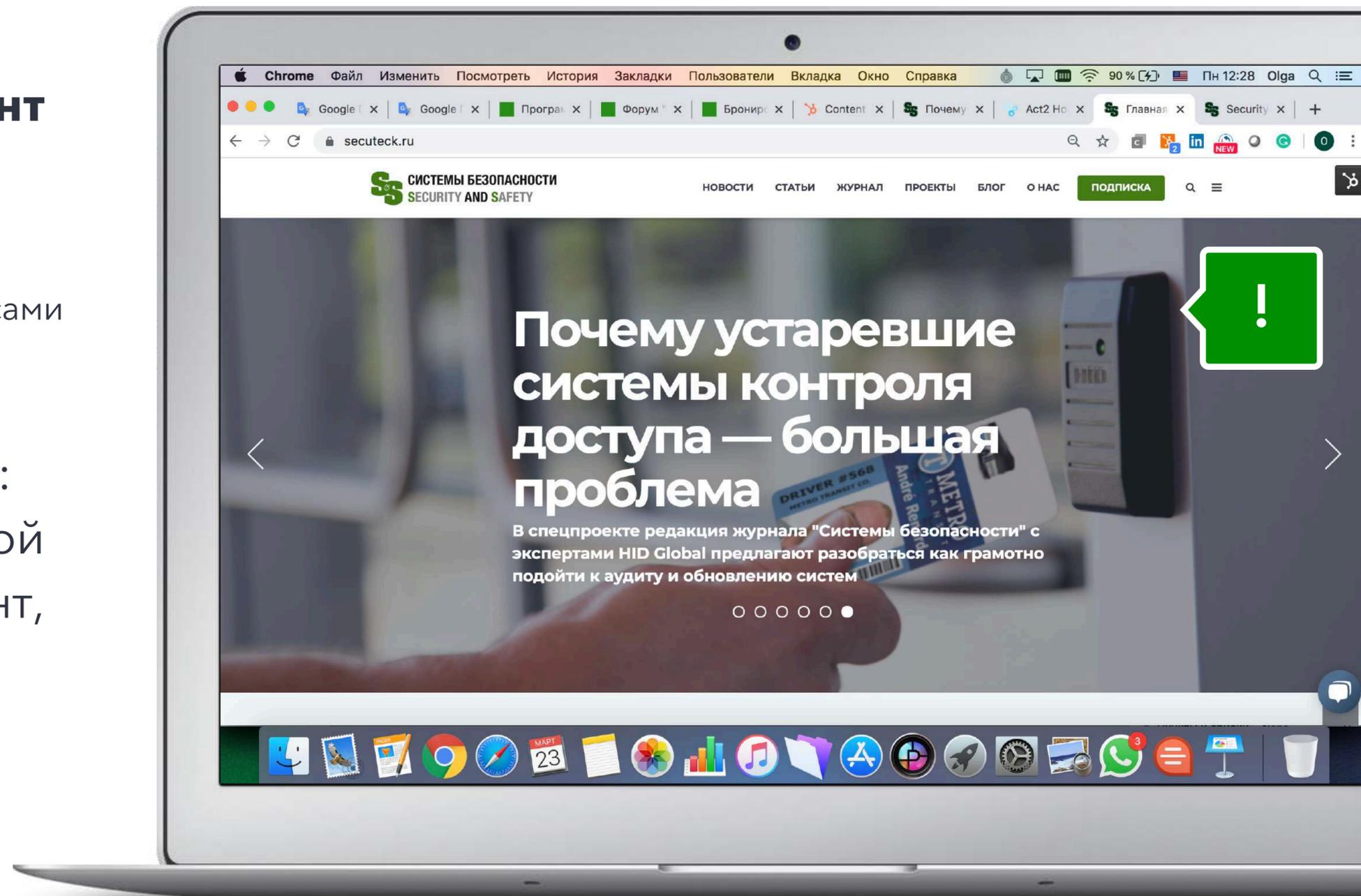
Мы возьмем у вас полезный контент

– White Paper – маркетинговый документ нерекламного характера.

Уже готовый в Pdf или Word. А можем и по частям сами скомпилировать для вас этот материал.

Через четыре недели вы получите:

- минимум **30 лидов** из вашей целевой аудитории, которые скачают документ,
- около **44 231*** просмотров вашего предложения на сайте Secuteck.ru



*Статистика посещений сайта secuteck.ru за март 2022

Что мы для этого делаем

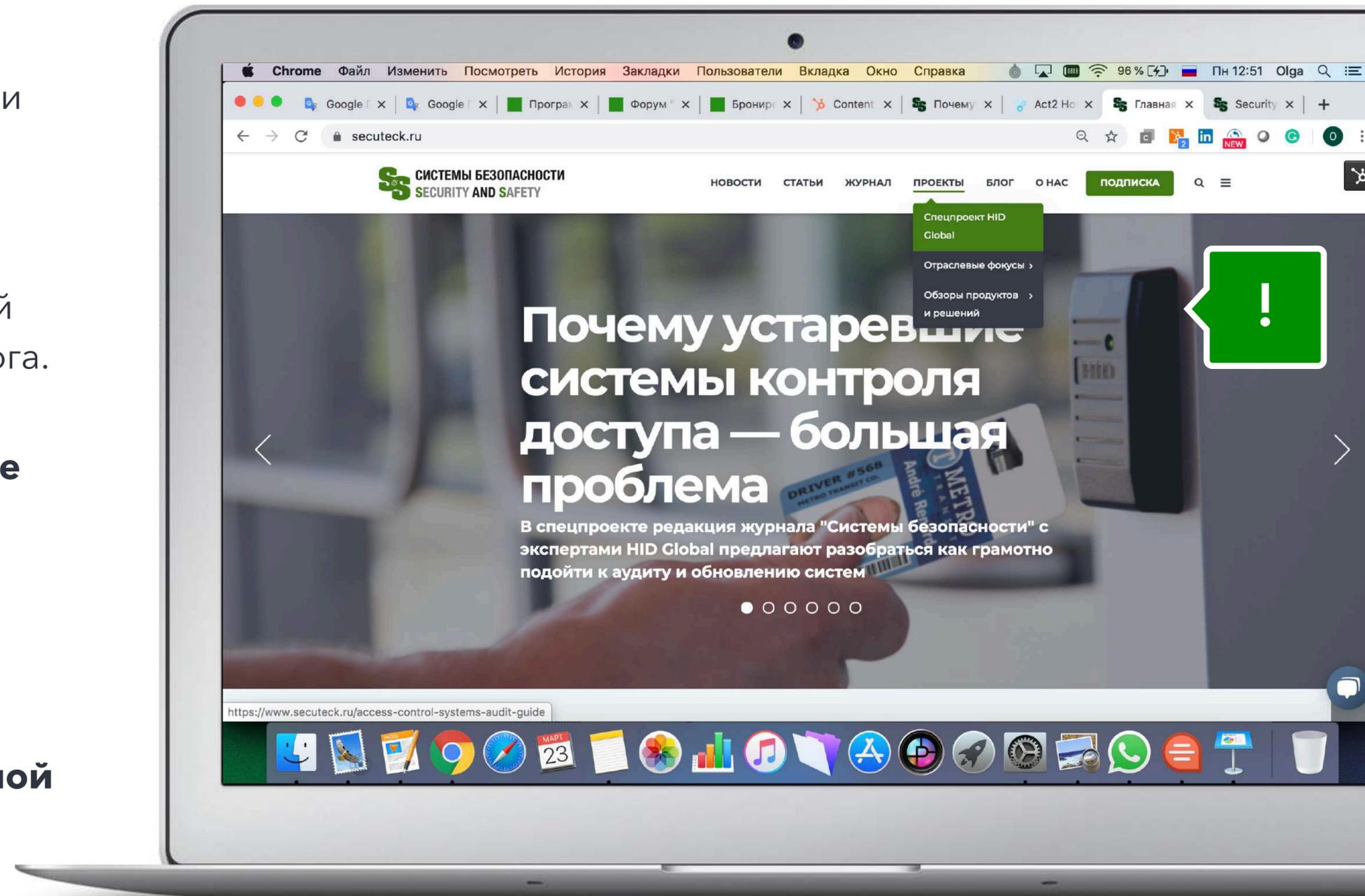
Создаем целевую страницу с формой генерации лидов и аргументацией, почему этот документ нужно скачать;

Пишем и публикуем пост в блоге secuteck.ru с еженедельными обновлениями и еженедельной автоматической рассылкой по подписчикам блога. Пост продвигается в доступных соцсетях (VK);

Ставим большой баннер на главной странице secuteck.ru в ротации;

Делаем сегментированные емейл рассылки в соответствии с профилем вашей целевой аудитории: например, по отраслям, интересам к продуктам;

Опубликуем часть материала **в виде экспертной статьи в журнале "Системы безопасности"**.



Какой контент подойдет

4

Любой полезный (= нерекламный) контент в виде:

- практических рекомендаций и гайдов,
- руководств и экспертных статей, отвечающих на вопросы что/как делать,
- лайфхаков или чек-листов,
- White Paper типа "задача-решение", который разбирает проблему и предлагает решение,
- "Результатов исследования", которые обобщают статистику о состоянии дел в индустрии или отдельном её сегменте,
- "Бэкграундера" – документа, который подробно рассказывает про преимущества технологии и ее использования.

Почему устаревшие системы контроля доступа являются большой проблемой

Современные системы контроля физического доступа позволяют избежать появления уязвимостей, имеют множество универсальных функций и закладывают фундамент для использования удобных мобильных средств идентификации.

КОНТРОЛЬ ДОСТУПА В ФИЗИЧЕСКИХ И ЦИФРОВЫХ СИСТЕМАХ ОДИНАКОВО ВАЖЕН, однако многие организации сегодня полагаются на устаревшие технологии и протоколы, из-за чего повышается вероятность хищения интеллектуальной собственности, нарушения конфиденциальности данных и несоблюдения стандартов безопасности. Специалисты по безопасности могут использовать такие события, как слияние и консолидацию компаний для проведения мероприятий по усовершенствованию систем контроля доступа с минимальными затратами денежных средств и минимальной потерей рабочего времени.

Согласно недавно проведенному исследованию, в котором участвовали почти 2000 членов всемирной ассоциации специалистов по безопасности ASIS International, многие системы контроля физического доступа (PACS) до сих пор используют устаревшую технологию карт-пропусков. Примерно половина используемых систем поддерживает низкочастотные (125 кГц) бесконтактные карты, а около трети — карты с магнитной полосой. И НЧ-карты, и карты с магнитной полосой легко можно подделать.

Старые уязвимые технологии контроля физического доступа позволяют злоумышленникам, преступникам и шпионам проникать на территорию охраняемых объектов или их частей, где они могут получить доступ к подключенным ко внутренней сети компьютерам, физическим ресурсам и (или) персоналу.

«Злоумышленник может без особого труда проникнуть сквозь эти старые системы контроля доступа, — заявил Брендон Арсемент (Brandon Arcement), директор по маркетингу HID Global. — Уязвимости — это реальная угроза. На рынке представлено огромное количество устройств, с помощью которых можно обмануть устаревшие системы контроля.»

ИДГ COMMUNICATIONS, INC.

Проблема заключается не только в ненадежных средствах идентификации. В системах контроля физического доступа входят считыватели карт и контроллеры. Обмен данными между ними осуществляется по соответствующему протоколу. Наиболее широко распространенный протокол, Wiegand, был создан в начале 1980-х. Он незашифрован и уязвим к технологиям внедрения и клонирования. Более того, такие устаревшие системы сложны и дороги в обслуживании, имеют ограниченный функционал и дистанции, их невозможно обновить удаленно.

Одним из существенных недостатков устаревших систем контроля физического доступа является также необходимость использования фирменного дорогостоящего ПО для существующей аппаратуры. Такая привязка к производителю ограничивает возможность организации выбирать поставщиков для повышения уровня безопасности, сокращения расходов и обеспечения удобства использования.

Системы контроля физического доступа не должны быть слабым звеном

Системы управления физическим и логическим доступом часто развивались независимо друг от друга, но за последние десятилетия некоторые продукты для контроля физического доступа были включены в ИТ-системы, а информационные технологии все шире применяются в процессах поставок, оценки и обслуживания решений для контроля физического доступа.

Таким образом, снижение рисков за счет объединения средств физического и логического доступа выходит на передний план, а технологии обеспечивают должный уровень безопасности. Смарт-карты второго поколения, например Seos², созданы с учетом возможности использования в различных сферах и позволяют управлять средствами идентификации независимо от базового оборудования.

Средства идентификации нового образца могут быть реализованы не только в виде карт, но и в виде программ для мобильных устройств, носимой электроники и в других форм-факторах. Кроме того, они могут передавать данные через NFC, Bluetooth и другие протоколы. Человек с меньшей вероятностью забудет мобильный телефон или носимую электронику дома, а их пропуск заметят быстрее в отличие от обычной карты-пропуска.

Замена физических средств идентификации цифровыми позволяет быстро реагировать на инциденты: отключать отдельные устройства и отзывать права доступа пользователей по беспроводным сетям. Также мобильные идентификаторы можно выдавать и обновлять в электронном виде, сокращая расходы и задержки, с которыми обычно связан выпуск пластиковых карт.

Не упускайте возможность обновления

Новые более динамичные технологии контроля доступа имеют ряд преимуществ перед более старыми и статичными. Успешный бизнес кейс для обновления системы создается вокруг трех ключевых преимуществ.

1. Повышенный уровень удобства в использовании и поддержка мобильных идентификаторов (в настоящем или будущем).
2. Высокая эффективность, снижение сложности управления картами, например в случае массовой замены карт.
3. Высокий уровень безопасности.

При наличии благоприятных условий специалисты по безопасности могут использовать ряд событий для реализации обновления систем.

- Обновление ИТ-сетей и инфраструктур позволяет гармонизировать системы, методы и процессы контроля физического и логического доступа за счет внедрения современных технологий, способных защитить инвестиции и повысить уровень безопасности.
- Слияние компаний дает возможность внедрить новые технологии, а не тратить бюджетные средства на интеграцию двух отдельных устаревших систем.
- Использование единого стандарта дает инструменты для централизованного управления надежными идентификаторами, обеспечивающие единообразие, безопасность и эффективность использования ресурсов.
- Консолидация, приобретение или перемещение производственных объектов требуют массового выпуска новых пропусков. В такой ситуации намного удобнее реализовать новый централизованный стандарт.

Почему устаревшие системы управления доступом являются большой проблемой

«ЗЛОУМЫШЛЕННИК МОЖЕТ БЕЗ ОСОБОГО ТРУДА ПРОНИКНУТЬ СКВОЗЬ ЭТИ СТАРЫЕ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА. УЯЗВИМОСТИ — ЭТО РЕАЛЬНАЯ УГРОЗА. НА РЫНКЕ ПРЕДСТАВЛЕНО ОГРОМНОЕ КОЛИЧЕСТВО УСТРОЙСТВ, С ПОМОЩЬЮ КОТОРЫХ МОЖНО ОБМАНУТЬ УСТАРЕВШИЕ СИСТЕМЫ КОНТРОЛЯ.»

Брендон Арсемент (Brandon Arcement), Директор по маркетингу HID Global.

*White Paper – маркетинговый документ нерекламного характера. Мощный инструмент контент-маркетинга, особенно популярный за рубежом.

Практический кейс. LP

5

Легенда кампании: редакция жСБ совместно с экспертами HID Global представляют специальный проект, в котором помогают выяснить, почему и как правильно обновлять системы контроля доступа. Статья будет опубликована в летнем выпуске журнала СБ, но вы можете скачать этот материал прямо сейчас

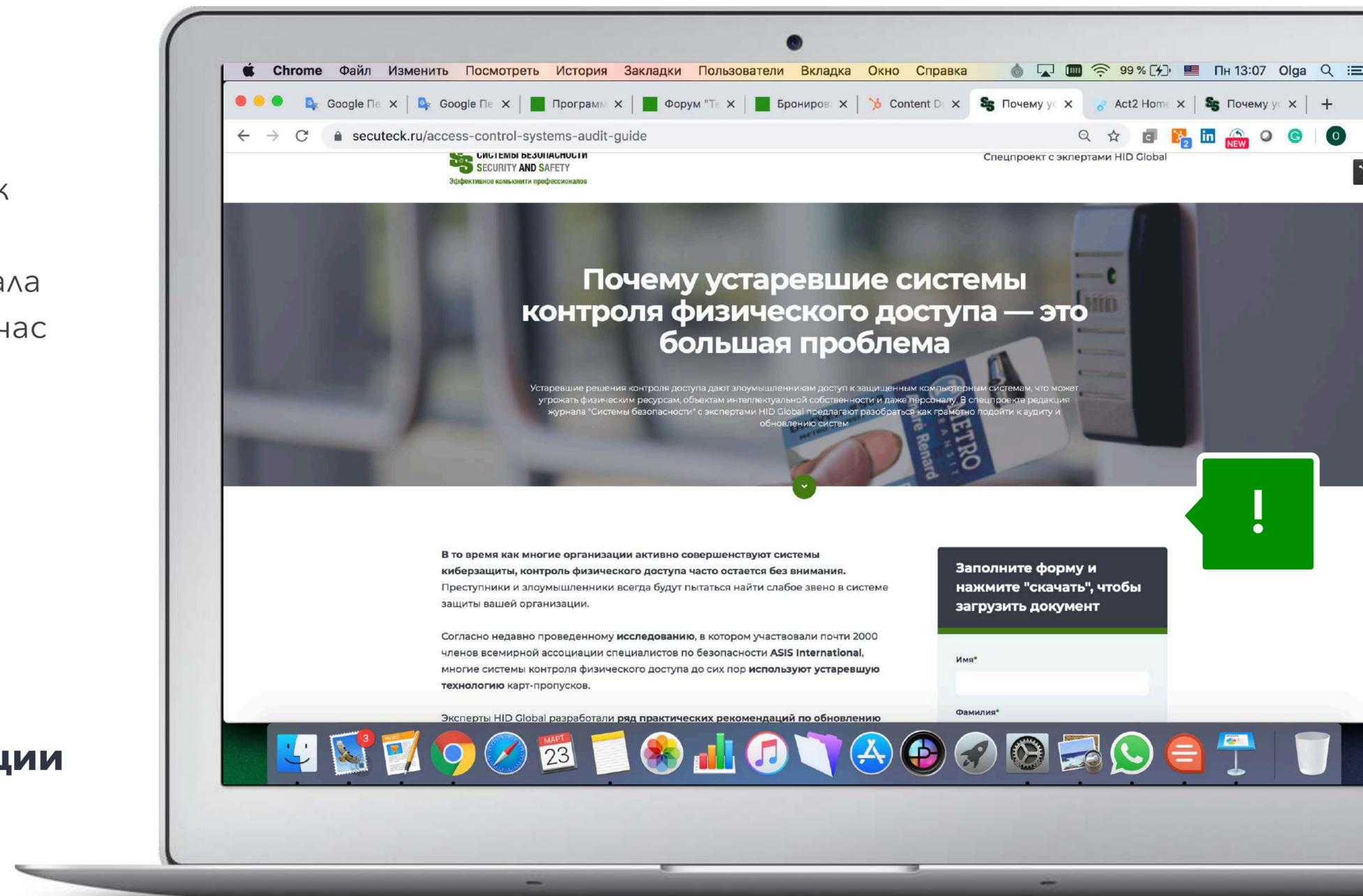
[Ссылка на страницу](#) для HID Global

Баннер на главной

Подменю в разделе проекты на главной

Две рассылки за период кампании

Мы гарантируем 30 лидов для каждой акции



*При необходимости включаем показ рекламных объявлений через Яндекс

Практический кейс. Блог

6

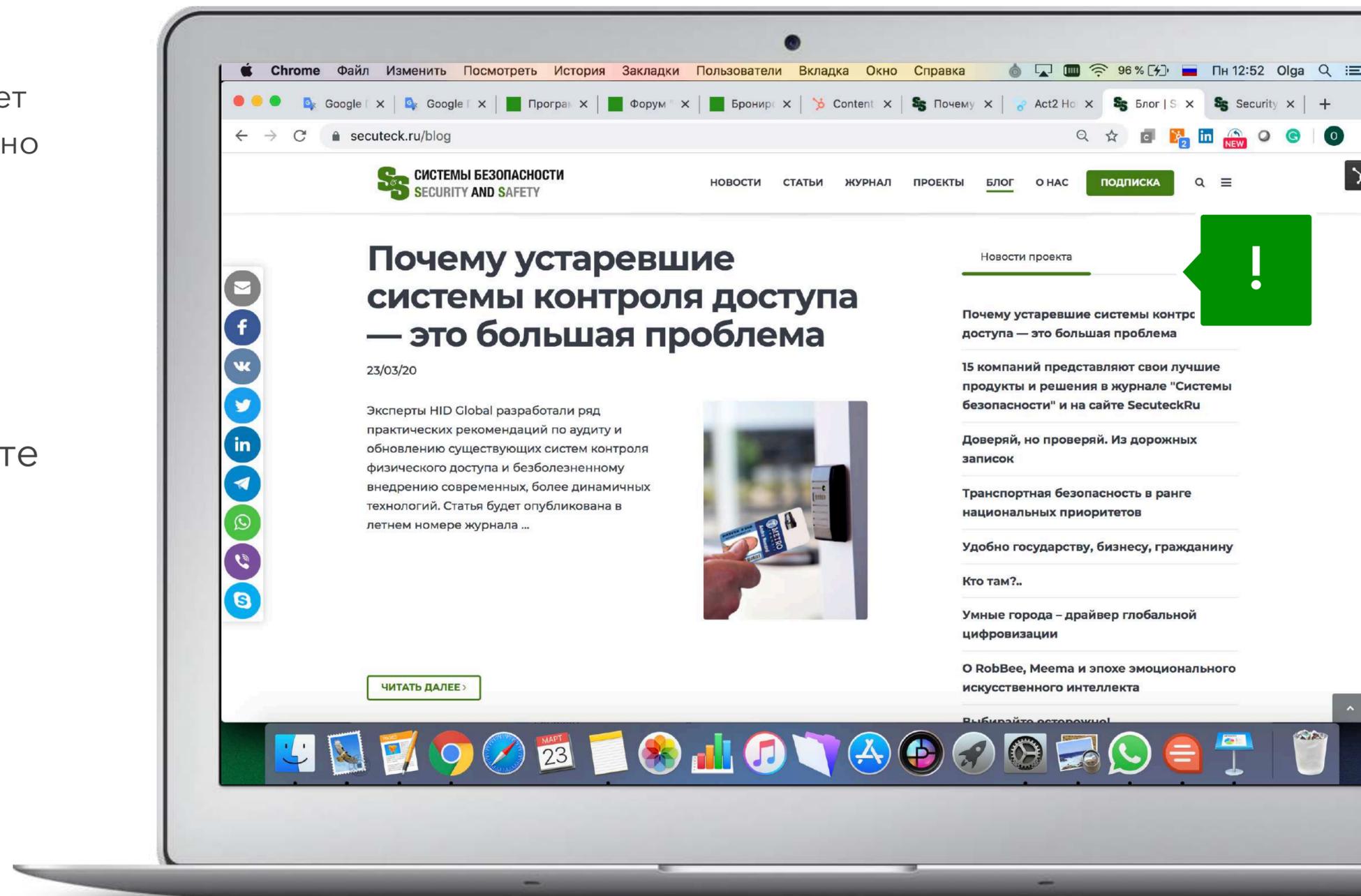
Редакция создает пост в блоге, в котором разъясняет что это за спец проект, в чем его ценность, как можно получить этот документ

[Ссылка на страницу](#) для HID Global

[Ссылка на текст поста](#) в блоге для HID

На картинке справа – вид в новостной ленте блога

Пост обновляется еженедельно в течение периода кампании

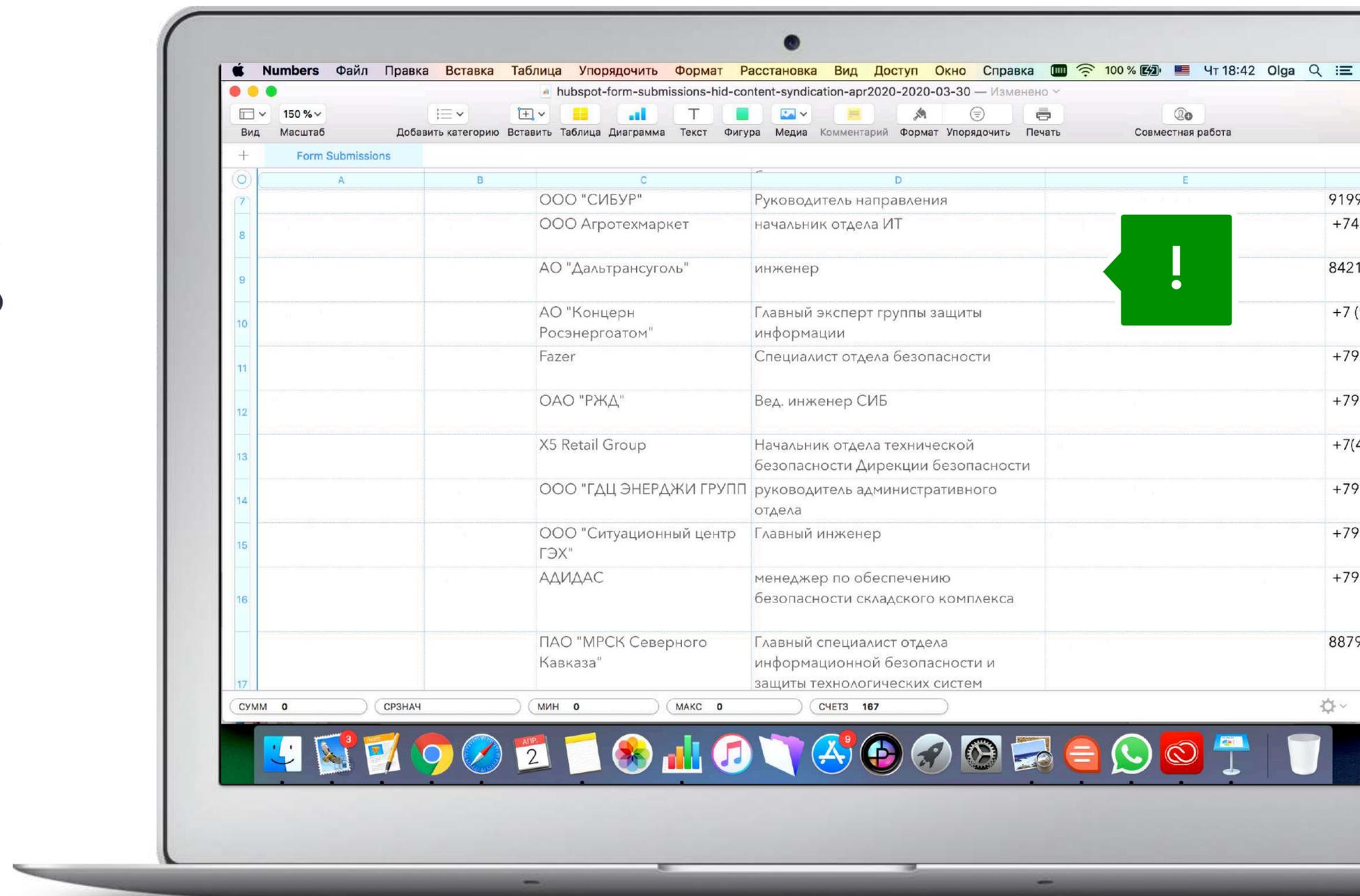


Практический кейс. Результат

7

Результат кампании:

- **57 лидов:** конечные заказчики из сферы транспорта, промышленности, нефтегаза и энергетики, банковского сектора и ритейла;
- **44 231*** просмотров вашего предложения на сайте [Secuteck.ru](https://secuteck.ru)



The screenshot shows a laptop screen with a spreadsheet application (Numbers) open. The spreadsheet is titled "Form Submissions" and contains a list of leads. The columns are labeled A through E. The data includes company names, titles, and phone numbers. A green speech bubble with an exclamation mark is overlaid on the spreadsheet, pointing to the contact information for the lead from "АО 'Дальтрансголь'".

	A	B	C	D	E
7			ООО "СИБУР"	Руководитель направления	9199
8			ООО Агротехмаркет	начальник отдела ИТ	+74
9			АО "Дальтрансголь"	инженер	8421
10			АО "Концерн Росэнергоатом"	Главный эксперт группы защиты информации	+7(
11			Fazer	Специалист отдела безопасности	+79
12			ОАО "РЖД"	Вед. инженер СИБ	+79
13			X5 Retail Group	Начальник отдела технической безопасности Дирекции безопасности	+7(
14			ООО "ГДЦ ЭНЕРДЖИ ГРУПП"	руководитель административного отдела	+79
15			ООО "Ситуационный центр ГЭХ"	Главный инженер	+79
16			АДИДАС	менеджер по обеспечению безопасности складского комплекса	+79
17			ПАО "МРСК Северного Кавказа"	Главный специалист отдела информационной безопасности и защиты технологических систем	8879

*Статистика посещений сайта secuteck.ru за март 2022

Стоимость услуги

8

Цель	Что входит в услугу	Период	Цена
Генерация лидов из целевой группы	<p>#1 Размещение маркетинговых нерекламных документов под скачивание</p> <p>#2 Создание страницы с формой для заполнения и сбора контактных данных</p> <p>#3 Написание текстов и публикация поста в блоге с еженедельным обновлением</p> <p>#4 Две рассылки со ссылкой на страницу с формой для скачивания</p> <p>#5 Не менее 30 полученных лидов</p>	3 недели	148 290 ₽

Все цены указаны без учета НДС

В сложных условиях санкционного давления и ограничения технологического сотрудничества с зарубежными компаниями мы делаем упор на цифровые услуги, которые помогут вам оставаться на связи со своими потенциальными клиентами, рассказывать о своих новинках, продуктах и решениях конечным заказчикам, обеспечивая регулярную и содержательную коммуникацию.

Используйте онлайн возможности, чтобы быть ближе к клиентам!

- ♦ платформа для регулярных коммуникаций с заказчиками
- ♦ контекстная реклама в Яндекс. Директ
- ♦ индивидуальные e-mail рассылки

Всегда на связи:
Наталья Матлахова

Руководитель проекта "Системы безопасности"
matlahova@groteck.ru

