



Совет ТПП МО
по цифровому развитию

Противодействие интернет-атакам на бренд и товарный знак

Практика защиты цифровых активов бизнеса и возможности
Совета ТПП МО по цифровому развитию

A night cityscape with a target overlay. The target consists of three concentric circles and a central dot, with a vertical and horizontal line intersecting at the center. The city lights are visible in the background.

Цифровые активы бизнеса под прицелом

Цифровой бренд компании сегодня — это не просто сайт или логотип. Это критически важная инфраструктура, атаки на которую наносят реальный финансовый, репутационный и правовой ущерб.

Эволюция угроз

Атаки сместились с чисто технического взлома на репутацию, бренды и доверие клиентов. Злоумышленники целенаправленно атакуют цифровую идентичность бизнеса.

Специфика фармации и медицины

Подделка сайтов — не только упущенная выгода, но и угроза жизни пациентов, компрометация врачебной тайны и санкции регуляторов.

Главная уязвимость

Отсутствие контроля за внешним цифровым периметром компании. Большинство организаций не знают, сколько клонов их сайта работает прямо сейчас.

Как злоумышленники атакуют бренды и фармкомпании

Современные атаки на бренд носят комплексный характер и воздействуют одновременно на технический, юридический и репутационный периметр компании.

Подделка доменов и фейки

Регистрация похожих доменов с приставками **-info**, **-pharma**, **-vip**. Полная или частичная копия интерфейса официального сайта. Пользователи не замечают подмены и взаимодействуют с мошенниками.

Сбор персональных данных

Несанкционированные формы обратной связи и «личные кабинеты» на клонах. Утечка ПДН: ФИО, контакты, чувствительная медицинская информация — с прямыми последствиями по 152-ФЗ.

Чёрный PR и дискредитация

Публикация ложных сведений о качестве медикаментов или оборудования. Риск расследований ФАС и долгосрочной потери доверия рынка и партнёров.

Реальный кейс: Рефлексия атаки и алгоритм защиты

ПРАКТИЧЕСКИЙ КЕЙС — INSTINCTOOLS

⚠ Проблема

Массовое клонирование посадочных страниц сайта **instincttools**. Злоумышленники регистрировали домены с приставками **-info** и **-vip**, полностью копируя оригинальный интерфейс.

- Скрытый сбор контактных данных клиентов без их ведома
- Прямой репутационный ущерб и компрометация бренда
- Реальная утечка персональных данных (ПДН) клиентской базы

✓ Решение и действия

Двухвекторная жалоба: одновременное обращение к **хостинг-провайдеру** и **регистратору доменов** через официальные саппорт-кабинеты.

- Использование официальных личных кабинетов провайдеров для подачи претензий
- Документирование нарушений: скриншоты, дампы, URL-адреса

✓ **Главный фактор успеха:** Наличие зарегистрированного Товарного Знака обеспечило быструю блокировку по факту нарушения исключительных прав.

Почему ТЗ — это фундаментальный элемент кибергигиены

Товарный знак — это не просто юридический документ. В эпоху цифровых атак это **главный операционный инструмент защиты**, определяющий скорость и стоимость нейтрализации угрозы.

✓ С зарегистрированным ТЗ

- Досудебная блокировка сайта или домена за **24–48 часов**
- Чёткое юридическое основание для хостинга и регистратора
- Минимальные затраты на нейтрализацию угрозы
- Прецедентная база для защиты в будущем

✗ Без зарегистрированного ТЗ

- Длительные судебные процессы или разбирательства в ФАС
- Необходимость доказывать факт недобросовестной конкуренции
- Продолжительный репутационный и финансовый ущерб, пока сайт работает
- Высокие юридические издержки без гарантии результата

Эффективный мониторинг цифрового пространства

Ручной поиск в Яндексе или Google не способен обнаружить современные фишинговые ресурсы — злоумышленники намеренно скрывают их от поисковой индексации и блокируют известные IP-адреса.



 Системы автоматизированного мониторинга сканируют соцсети, Telegram-каналы, форумы и СМИ в режиме 24/7, фиксируя угрозы задолго до того, как они наносят ущерб.

4 шага к комплексной защите

- Регистрация ТЗ

Оформить права на бренд, названия ключевых продуктов и препаратов, графические элементы. Это фундамент всей системы защиты.

- Сквозной мониторинг

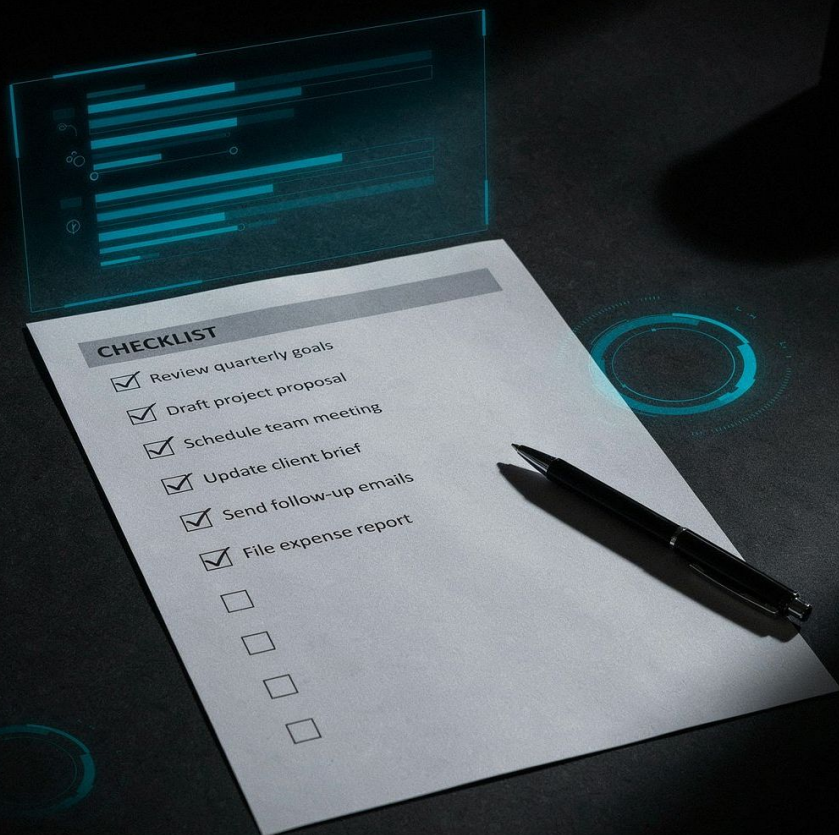
Внедрить системы аналитики соцмедиа и мониторинг новых доменных регистраций, схожих с вашим брендом, в режиме реального времени.

- Разработка плана действий

Утвердить регламент быстрых действий при обнаружении клона: чёткое распределение ролей между юристами, PR-командой и IT-службой.

- Взаимодействие с экспертами

Использовать ресурсы и платформу Совета ТПП МО по цифровому развитию для доступа к экспертизе, методологии и экосистеме партнёров.



Ваша точка опоры в вопросах цифровой безопасности

Совет ТПП МО по цифровому развитию объединяет экспертизу, правовые инструменты и отраслевые связи для системной защиты бизнеса Московской области в цифровом пространстве.



Методологическая поддержка

Помощь в разработке регламентов реагирования на киберугрозы и атаки на бренд. Готовые шаблоны Playbook и чек-листы для быстрого развёртывания.



Экспертный консалтинг

Анализ рисков и правовая поддержка при защите интеллектуальной собственности. Сопровождение споров с хостинг-провайдерами и регуляторами.



Синергия с экосистемой

Взаимодействие с отечественными разработчиками ИБ-решений, включая АРПП «Отечественный софт», и профильными регуляторами для комплексной защиты.



Информационный хаб

Системная работа по защите интересов бизнеса Московской области: мониторинг угроз, обмен лучшими практиками и оперативное информирование участников.

СОВЕТ ТПП МО ПО ЦИФРОВОМУ РАЗВИТИЮ



Совет ТПП МО

по цифровому развитию

Карпов Максим Владимирович

Заместитель председателя Совета ТПП МО по цифровому развитию

+7 903 299-99-97

mk@digitalmosobl.ru

Начните с независимой экспертной оценки задачи — без обязательств для предприятия.

Совет ТПП МО

Единое окно для промышленных предприятий:
экспертиза, решения, сопровождение