



АКТУАЛЬНЫЕ КИБЕРРИСКИ

И МЕТОДЫ ИХ ПРЕДУПРЕЖДЕНИЯ

Игорь Бедеров

Председатель совета по противодействию
технологическим правонарушениям

КС НСБ России

Регуляторные риски:

включение **всех субъектов бизнеса**
в число операторов персональных данных.



СУТЬ:

Оборотные штрафы за утечки персональных данных, а также повышение штрафов за неуведомление о факте утечки, сделали защиту информации вопросом выживания бизнеса.



ЧТО НЕОБХОДИМО:

Обеспечивать базовый уровень информационной безопасности.

- Ведение киберразведки.
- Выявление утечек данных, программного кода и ключей API.
- Нарушение парольной политики.
- Проверка наличие уязвимостей собственной инфраструктуры.
- Управление инцидентами утечек и компрометации исходного кода.



Регуляторные риски:

перенос ответственности за действия
интернет-мошенников на действующие
компании.



СУТЬ:

Разъяснения Верховного Суда РФ (дело № 5-КГ25-30-К2) возложили на компании материальную ответственность за мошенничества, совершенные от их имени с использованием сайтов-двойников. Доказывать непричастность к таким ресурсам обязана сама организация, а не потребитель.



ЧТО НЕОБХОДИМО:

организовать и вести мониторинг предложений своих товаров и услуг от третьих лиц (мошенников).

Сюда входят:

- сквоттинг доменов и социальных сообществ,
- копирования фирменного стиля сайтов,
- удаление и блокировка мошеннических ресурсов.



Репутационные **риски**



СУТЬ:

Автоматизированный мониторинг публичного поля для раннего обнаружения недостоверной, компрометирующей информации и вбросов, способных нанести репутационный и финансовый ущерб.



ЧТО НЕОБХОДИМО:

Интеграция мониторинга информационного поля в контур защиты активов.
Превращение мониторинга упоминаний из PR-функции в аналитический инструмент раннего предупреждения атак СБ.



Атаки БПЛА, диверсии и завербованные сотрудники



СУТЬ:

Физические атаки могут быть детектируемы через различные инструменты кибербезопасности.



ЧТО НЕОБХОДИМО:

- Формирование единого контура безопасности (СБ + ИБ). Безопасность перестает быть «силовым придатком» и становится аналитическим центром управления рисками. Для этого ей необходим инструментарий, традиционно относившийся к сфере ИБ: OSINT, киберразведка, мониторинг даркнета и прогнозная аналитика.
- Пересмотр программ повышения осведомленности сотрудников в области кибератак через сеть Интернет и в физическом мире. Регулярные тренировки и сдача зачетов.
- Введение обязательных инструктажей при приеме на работу и периодических.



СПАСИБО ЗА ВНИМАНИЕ!



Игорь Бедеров

Председатель совета по противодействию
технологическим правонарушениям
КС НСБ России

