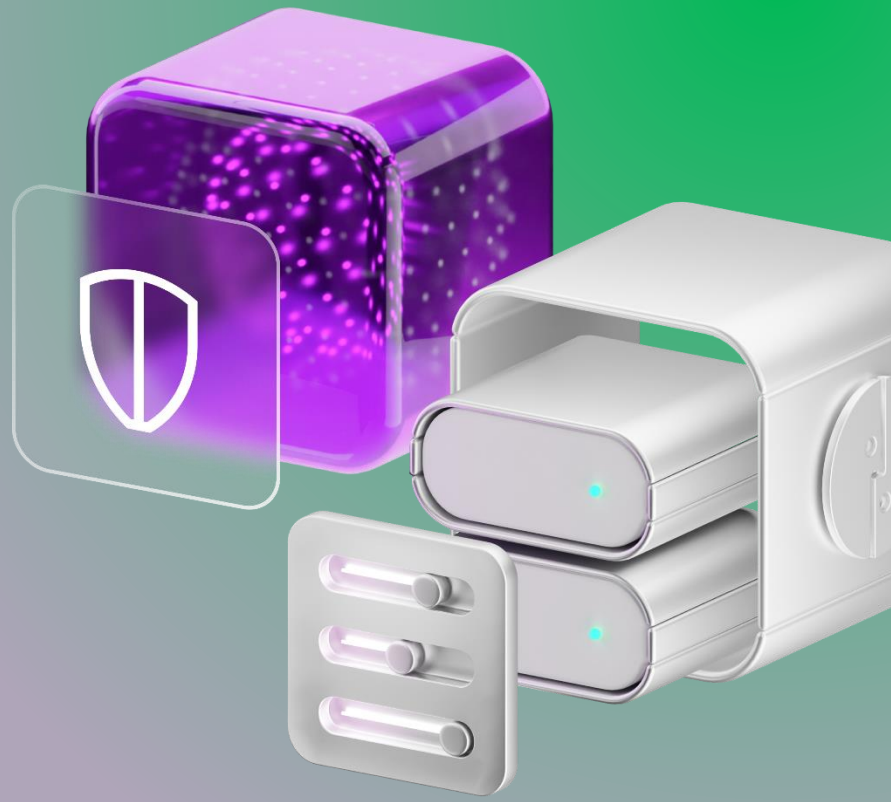
МЕГАФОН | ПроБизнес

Рискориентированный подход к информационной безопасности



МЕГАФОН | ПроБизнес

Как сейчас вы согласовываете бюджет по ИБ?

Что мы сейчас видим?

1. Решения ИБ комплексно внедряются крайне редко
2. Внедрение происходит точечно и в большинстве случаев после инцидента
3. Соответствие требований регуляторов
4. Проведение анализов защищенности (положительная динамика)

ПроБизнес

С чего начать?

1

Инвентаризация активов

Проведение учета, фактического наличия и состояния материальных и не материальных активов организации

2

Определить их ценность и значимость

Оценка вероятной стоимости и значимости выявленных активов

3

Определить перечень потенциальных рисков

Определение перечня потенциальных рисков кибербезопасности

4

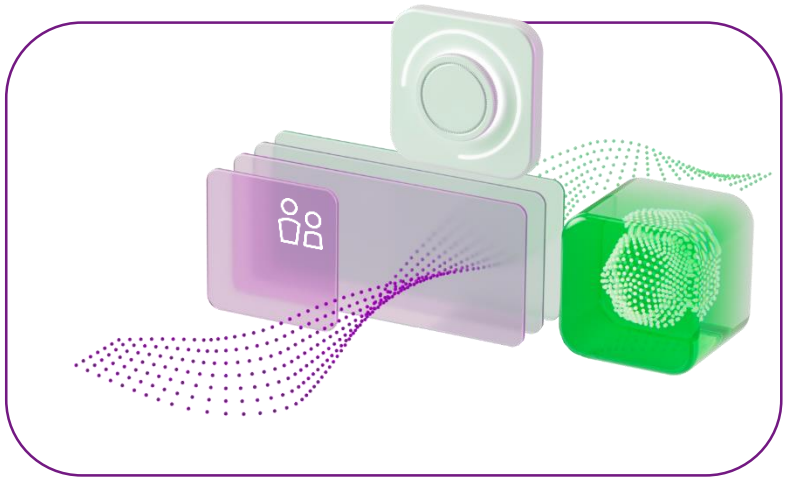
Вероятность возникновения риска

Вычисление потенциальной вероятности наступления определенного перечня рисков

5

Обработка оцененных рисков

Оценка вероятных материальных потерь и имиджевых рисков

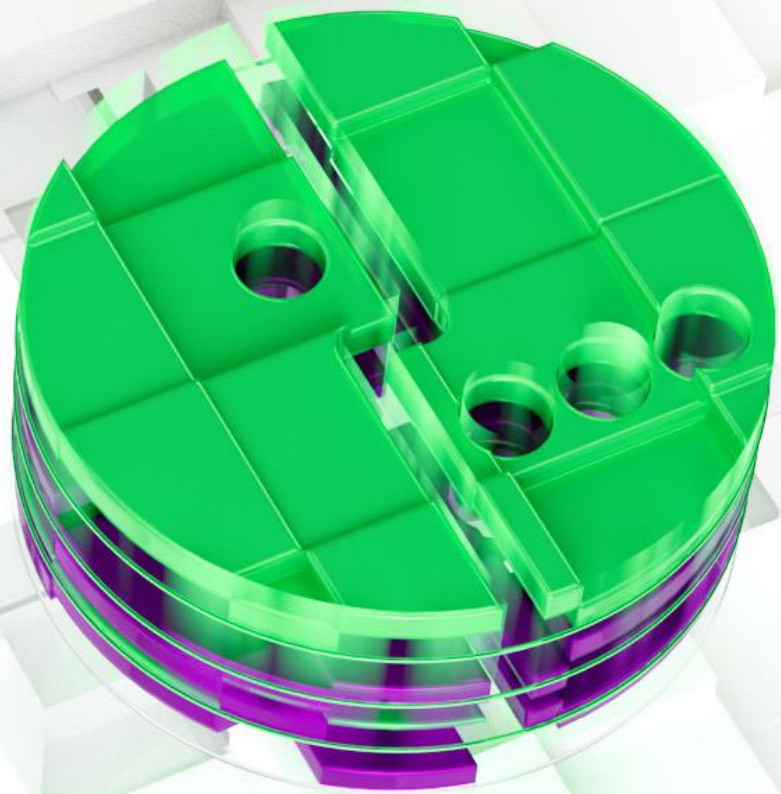


МегаФон | ПроБизнес

Давайте разбираться на примере

Компания занимается производством и продажей автомобильных аксессуаров

Есть собственная торговая сеть в разных регионах, онлайн-магазин, доставка, а также сеть партнеров (франшиза)



ПроБизнес

Инвентаризация активов

Материальные

Программное и аппаратное обеспечение, платформа, устройство

Нематериальные

Информация, данные, торговая марка, лицензия, патент, интеллектуальная собственность, репутация

Материальные:

- Серверное оборудование/СХД
- Виртуализация, ОС
- Прикладное ПО (CRM, АСУ ТП, Офисные приложения)
- Производственное оборудование
- Облачная платформа
- Сетевое оборудование

Нематериальные:

- Базы данных покупателей
- Данные о партнерской сети
- Внутренние данные по бизнес-процессах
- Финансовые данные
- Информация о новых разработках

Примерный перечень рисков

Внешние клиенты (потенциальный злоумышленник, бот)

Сетевая уязвимость

Взлом подрядчика

Подрядчики (разработчики)

WAF

NGFW

Веб-ресурсы, CRM, онлайн-сервисы

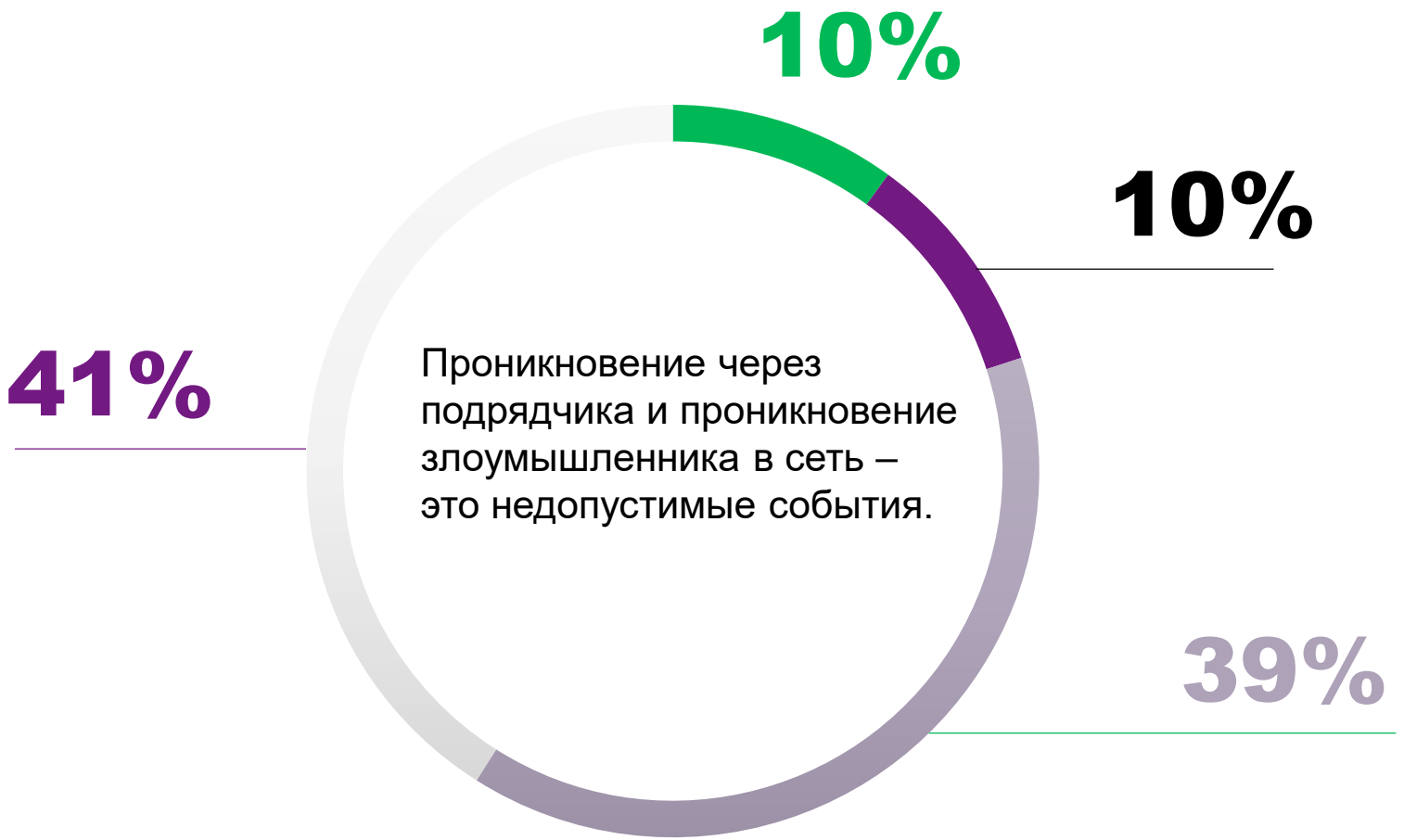
Обновление ПО

Нет полноценного контроля

KSC, DLP, маршрутизаторы, AD

Обновление ПО

Вероятность



Обработка рисков

Риск 1: Подрядчик, проникновение в инфраструктуру производства

Данное признано неприемлемым и повлечет репетиционные и финансовые потери

Примерная стоимость потери активов = ~95 млн руб

Репутационные риски = отказ всех партнеров от франшизы (это 4 региона) + публикация в СМИ.

Внедрение:

PAM решения, SA (для подрядчика), двухфакторная аутентификация. = ~25 млн руб. в год.

Риск 2: Проникновение в сеть и получение доступа ко всей инфраструктуре

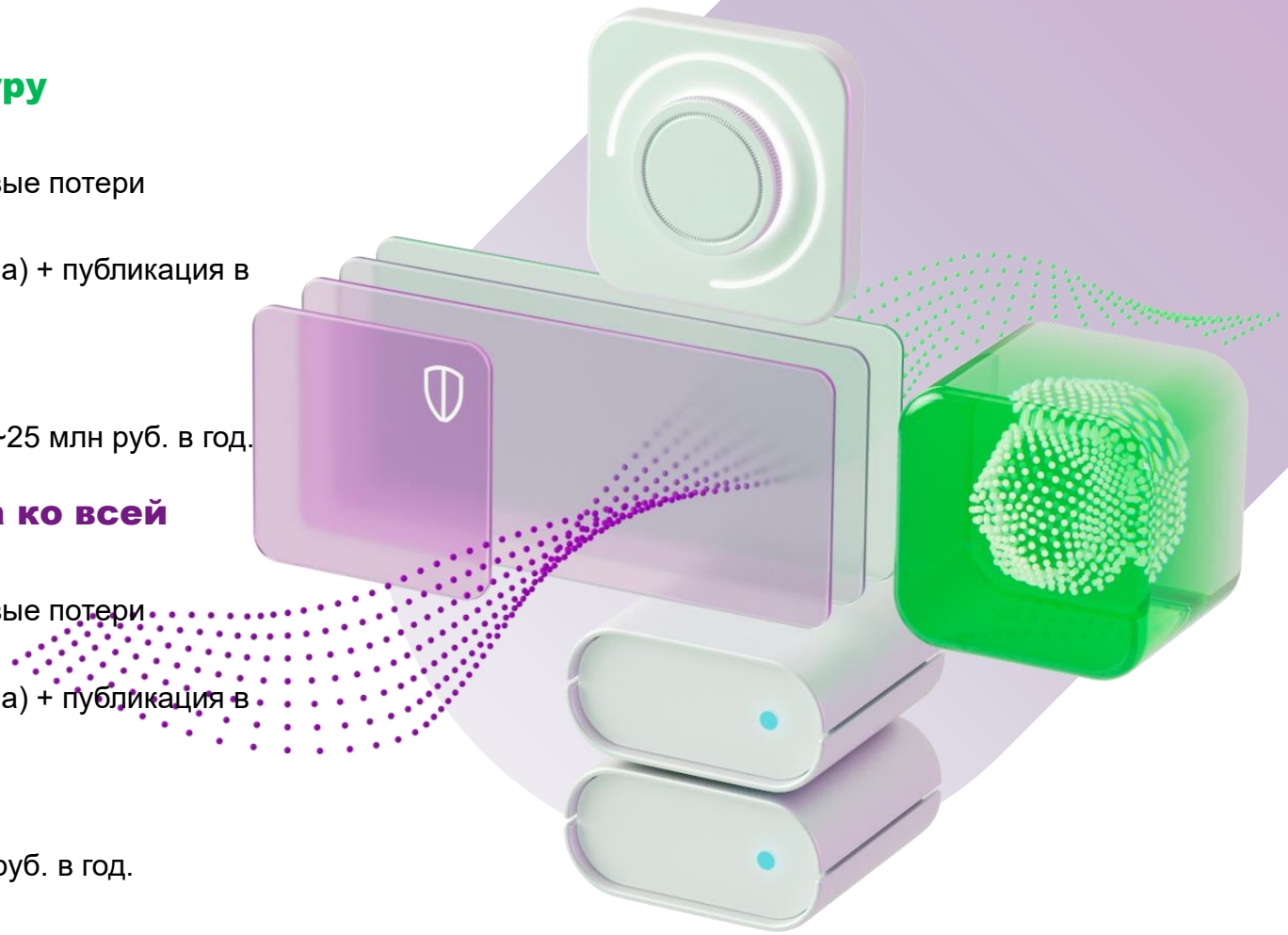
Данное признано неприемлемым и повлечет репетиционные и финансовые потери

Примерная стоимость потери актива = ~230 млн руб

Репутационные риски = отказ всех партнеров от франшизы (это 4 региона) + публикация в СМИ.

Внедрение:

ПО для глубокого анализа трафика, ЗБД, СЗИ от НСД, SIEM, = ~45 млн руб. в год.



Выводы

Внедрение всех подряд решений ИБ будет дороже стоимости активов

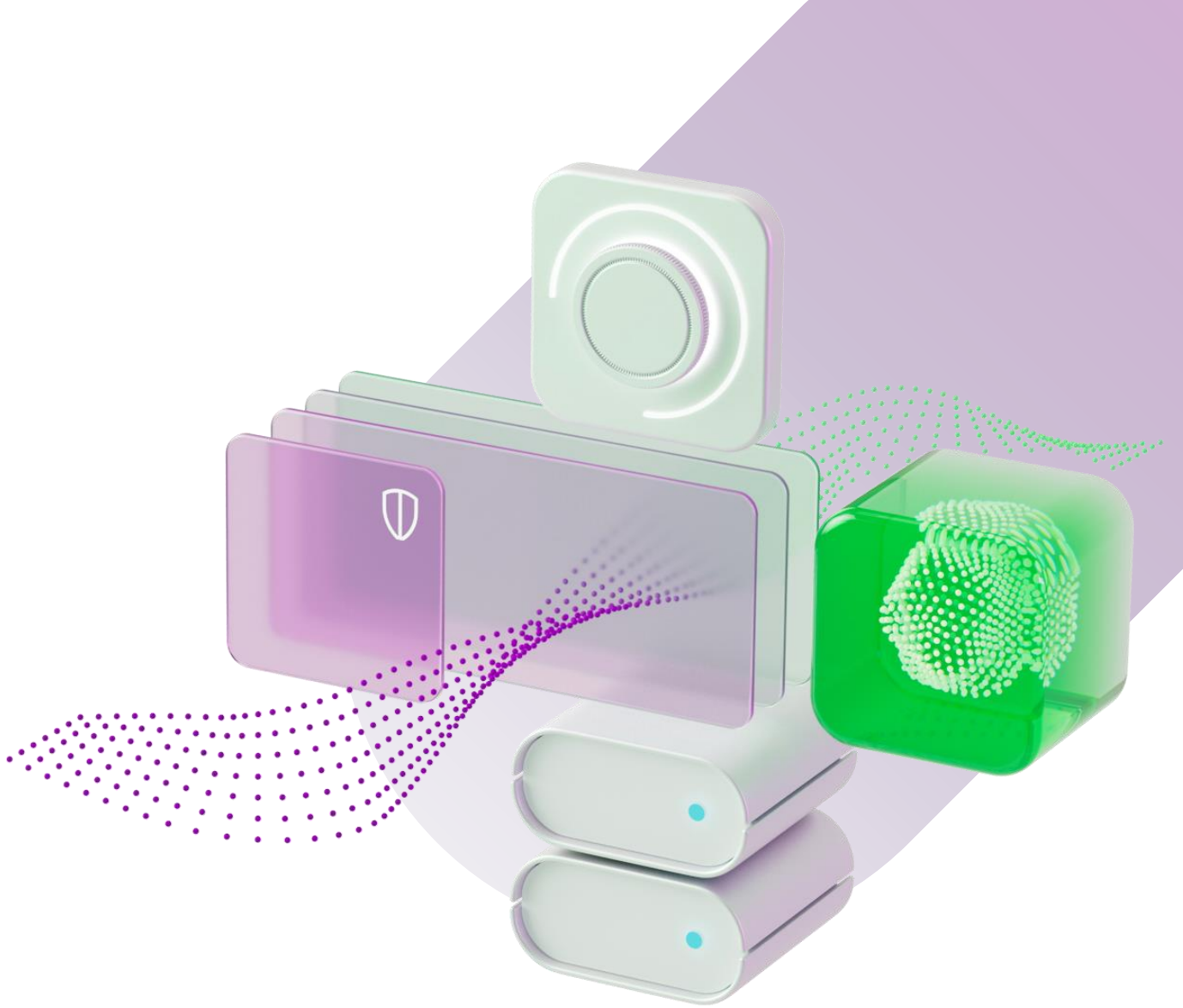
~230 млн – стоимость активов

~348 млн – стоимость решений ИБ

При внедрении риск-ориентированного подхода

~230 млн – стоимость активов

~70 млн – стоимость решений ИБ



МегаФон | ПроБизнес

Сергей Мешков

Руководитель направления по внедрению цифровых решений Урал и Центр