ПСБ банк для бизнеса

июнь 2026

Стратегический аутсорсинг кибербезопасности:

Когда отдавать и что оставить внутри?

Сафрон Дандаев

Директор по развитию сервисов кибербезопасности

Куда ИБ тратит деньги?

1. На защиту Банка

1. Выполнение требований регуляторов

1. Оборотные штрафы:
За утечку персональных данных (ст. 13.11 КоАП РФ) штрафы исчисляются уже миллионами. Появились оборотные штрафы (до 3%).

2. Многочисленные регуляторные ограничения:
ФЗ-152 «О персональных данных», ФЗ-149 «Об информации», ФЗ-187 «О безопасности КИИ», ФЗ-395-1 «О банках», Положение ЦБ № 683-П (защита переводов), Положение ЦБ № 728-П (СУИБ), Указание ЦБ № 5648-У (инциденты и ФинЦЕРТ), Приказы ФСТЭК (№21, 239) и Постановление Правительства № 1119 , требования ФСБ России и т.д.

3. Уголовная ответственность:
Согласно ст. 274.1 УК РФ за нарушение правил эксплуатации средств хранения данных критической инфраструктуры предусматривается реальная уголовная ответственность

2. На развитие и реальную защиту

1. **Повышение эффективности защиты (качество детектирования угроз, ускорение реагирования)**
   - платформы нового поколения (AntiDDos, NDR, EDR, WAF, SOC-платформы)
   - импортозамещение инфраструктуры БИБ
   - лицензии и подписки на платные сервисы, TI-фиды и т.д.
2. **Автоматизация процессов команд ИБ для снижения операционных расходов**
   - SOAR (оркестрация плейбуков)
   - роботизация задач аналитиков и экспертов
   - DevOpsSec-пайплайны

2. На защиту клиентов Банка

1. Антифрод (безопасность платежей)

Повышение эффективности аналитических платформ с поведенческими алгоритмами и скорингом транзакций в реальном времени

2. Threat Intelligence (TI) — разведка угроз

Осуществляется ежедневный мониторинг десятков теневых каналов, даркнета и фишинговых сетей.

и множество других направлений обеспечения ИБ

Стоимость и экономика

Прямые расходы
Скрытые траты

2. Экспертиза и качество

Стратегический аутсорсинг кибербезопасности

Когда отдавать, чтобы усилить контроль, а не потерять его?

Аутсорсинг — это не потеря контроля, а перераспределение фокуса на бизнес-риски.

Место, чтобы разместить источники

Предлагаемая модель

«Ядро — Оставить. Периферия — Отдать»

Что зачастую стратегически выгодно отдать

1. 24/7 SOC (мониторинг) — дешевле штата из 5–8 человек на смену, лучше покрытие.

2. Пентесты и Red Teaming — нужен свежий взгляд «со стороны» (не ваш внутренний сисадмин).

3. Облачная безопасность + резервное копирование.

Место, чтобы разместить источники

Российские особенности: регуляторика и доверие

ФСТЭК и Банк России не запрещают MSSP, но **ответственность за инцидент несет юр. лицо**.

Локализация: аутсорсер должен быть аттестован и иметь лицензии на деятельность

Запрет на иностранные MSSP

Главный вывод: бизнесу больше не важно, как называется исполнитель — важно, снижает ли он риски и ущерб в рамках бюджета.

Место, чтобы разместить источники

ПСБ банк для бизнеса

06.2026

Спасибо за внимание

Сафрон Дандаев

Директор по развитию сервисов кибербезопасности