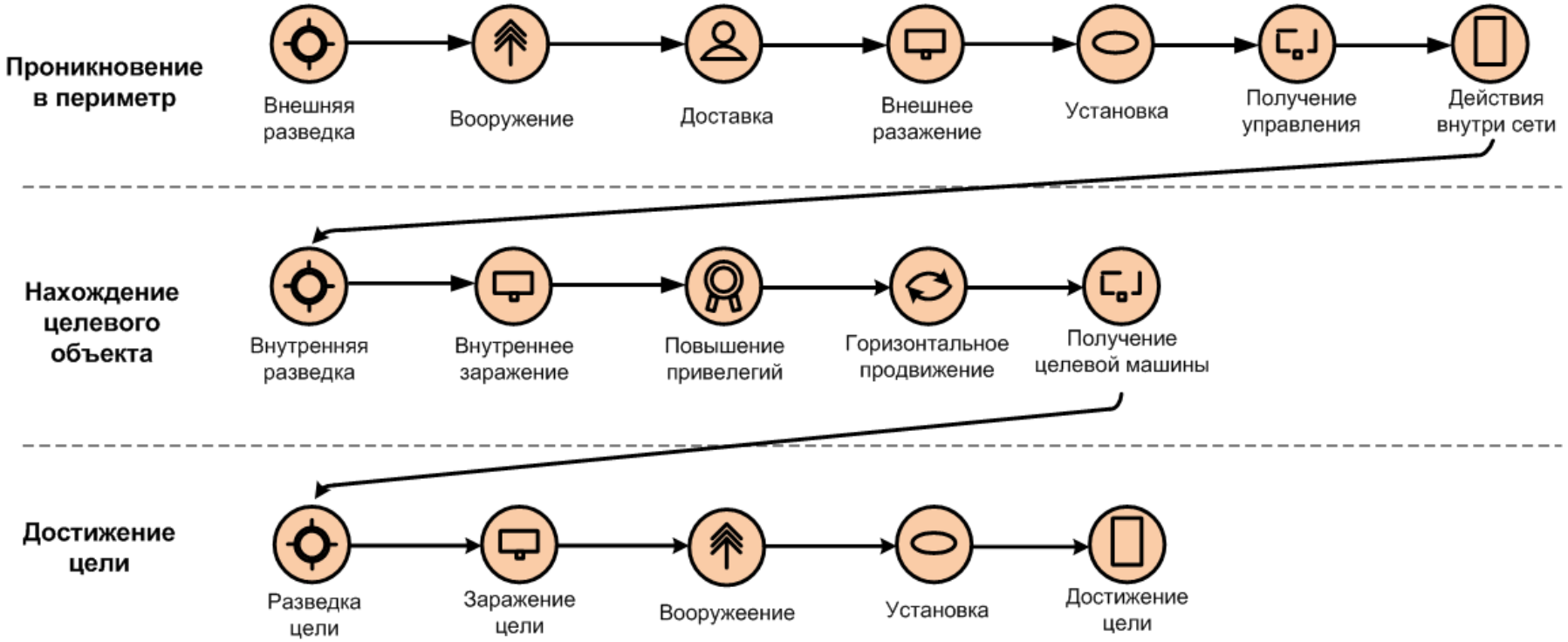
Механизмы противодействия кибератакам

абсолют банк

Кто такие злоумышленники

	Злоумышленники	Цели	Инструменты
1	Автоматизированные системы	Парсинг, сканирование хостов, разведка для последующей перепродажи данных	Автоматизированные сканеры
2	Одинокие хакеры / хулиганы	Хулиганство, нарушение целостности инфраструктуры	Коммерческие и свободно распространяемые инструменты
3	Киберкриминал / Организованные группировки	Майнинг, шифрование данных, ботнеты, фишинг, монетизация результата	Кастомизированные инструменты, свободно распространяемое вредоносное ПО, известные уязвимости
4	Кибернаемники / Продвинутые группировки	Заказные работы, шпионаж в интересах заказчика, крупная монетизация результата, разведка, хактивизм	Самостоятельная разработка инструментов, приобретенные zero day и уязвимости
5	Группировки спонсируемые государствами	Кибершпионаж, захват и контроль инфраструктуры, хактивизм, любые действия	Самостоятельный поиск zero day, самостоятельная разработка и внедрение закладок

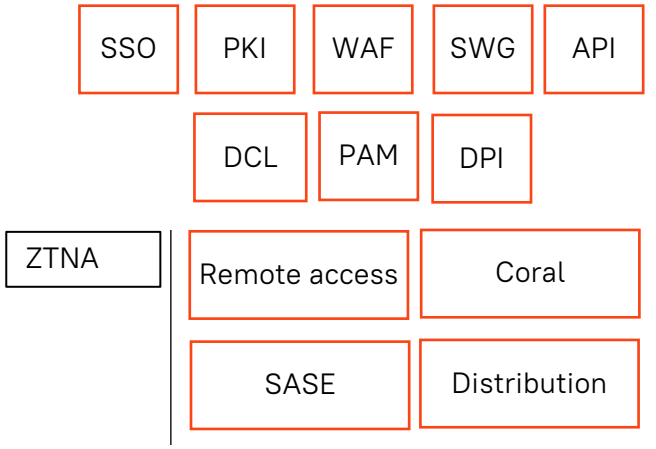
Как происходит атака



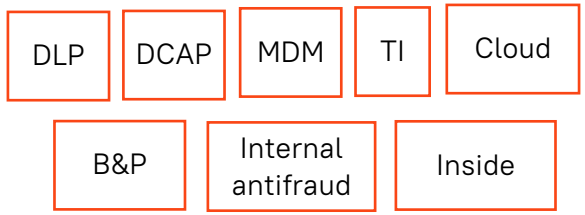
Безопасность как экосистема

1. Управление инцидентами

2. Сетевая безопасность

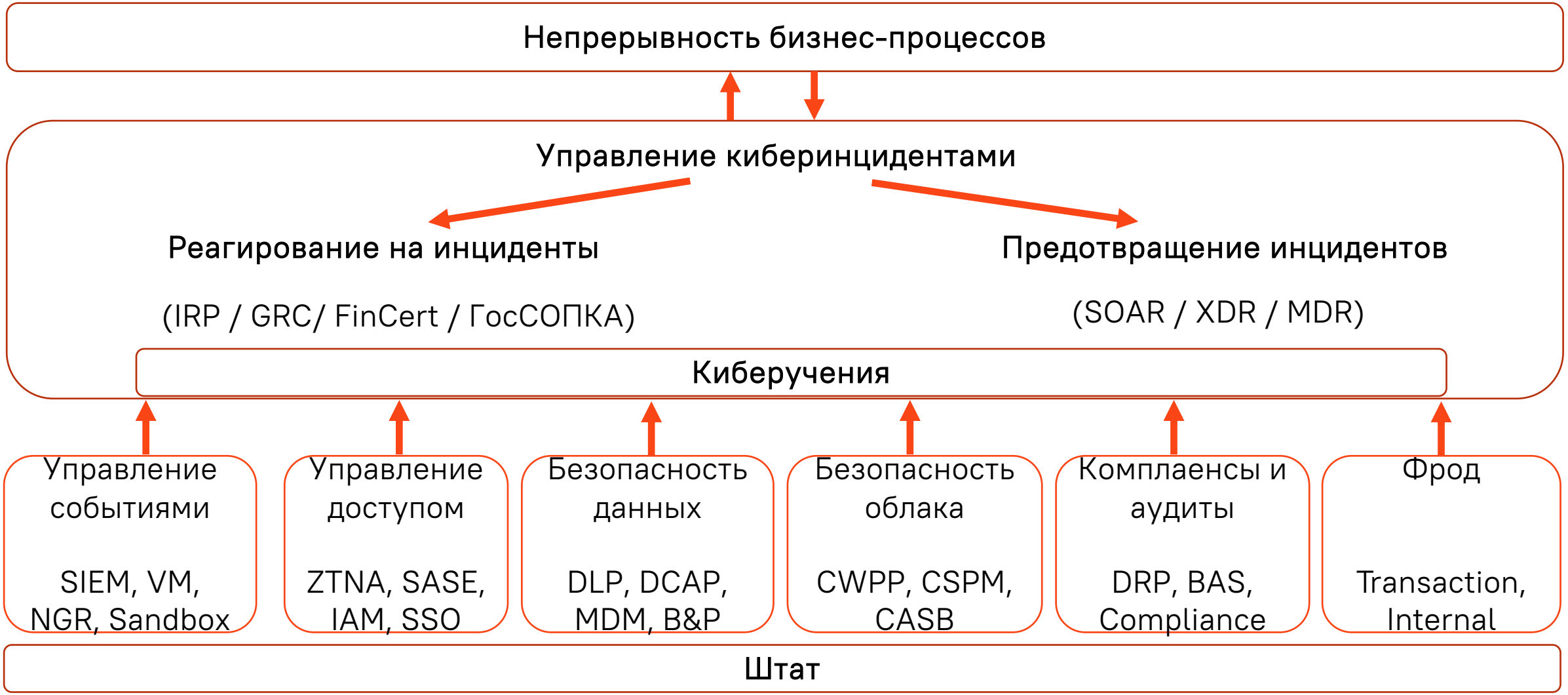


3. Защита данных

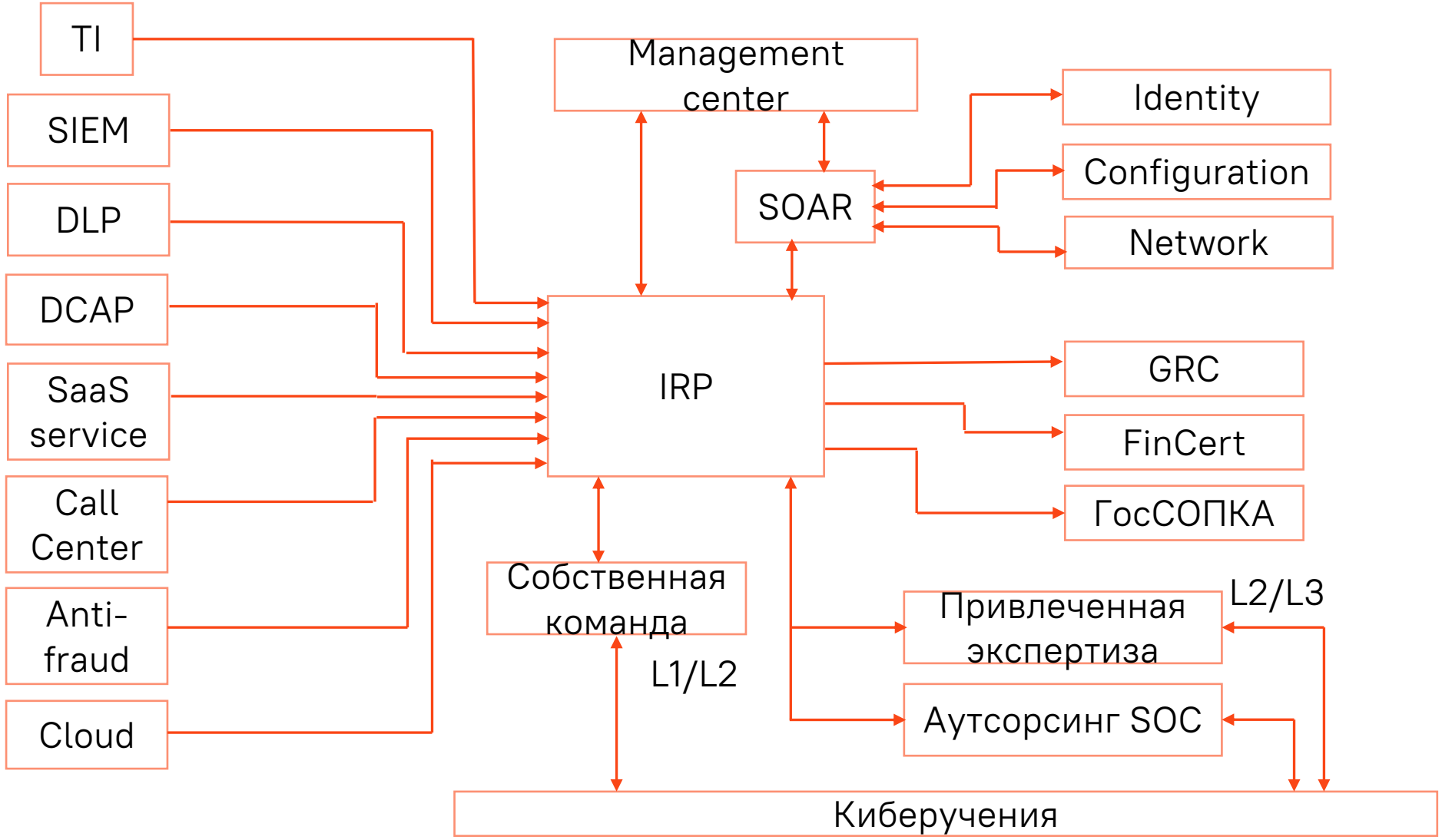


4. Безопасность облачных сред

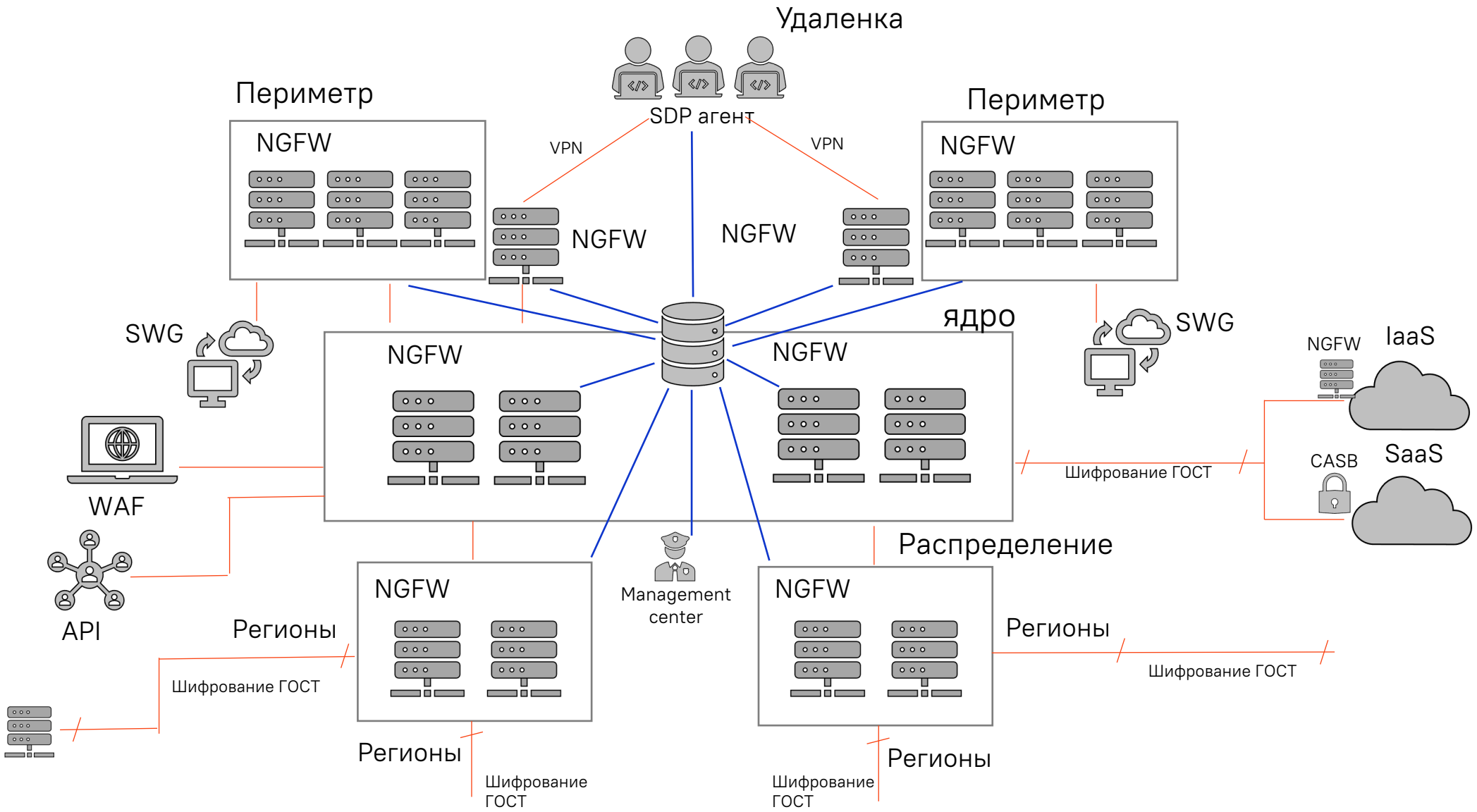
1. Управление инцидентами



Модель гибридного SOC

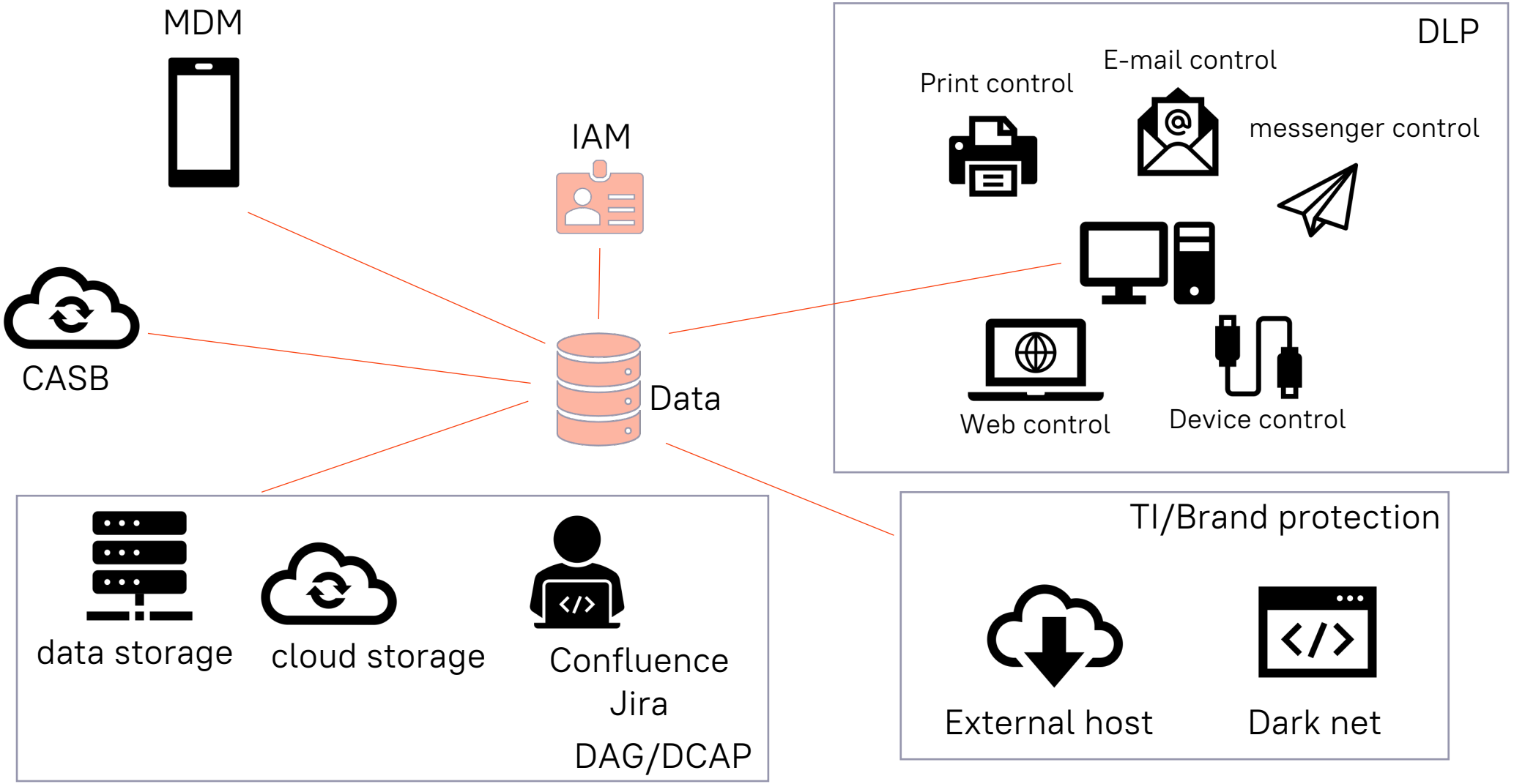


2. Безопасность сети



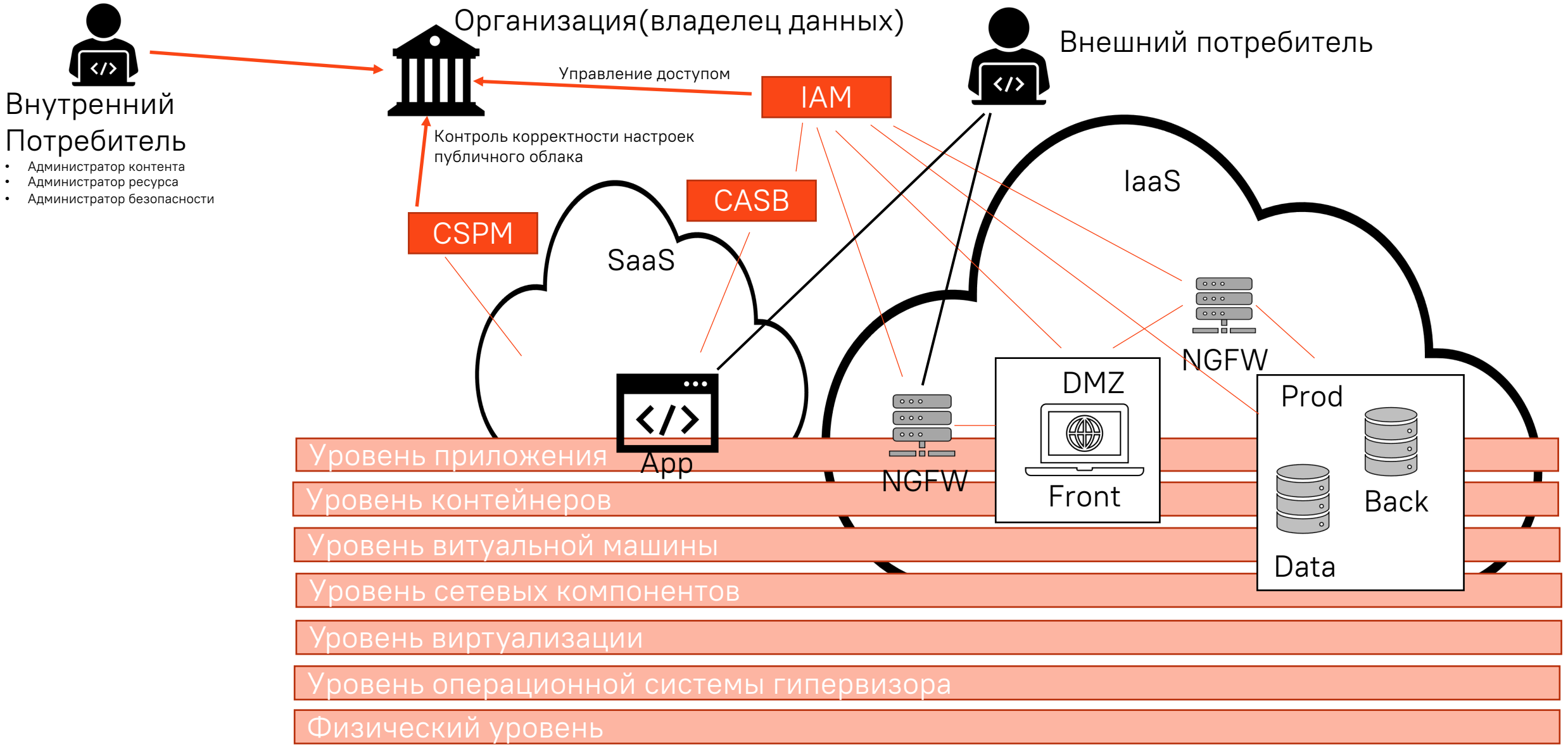
3. Защита данных

Данные на рабочих местах, не структурированные данные, мобильные данные, утекшие данные

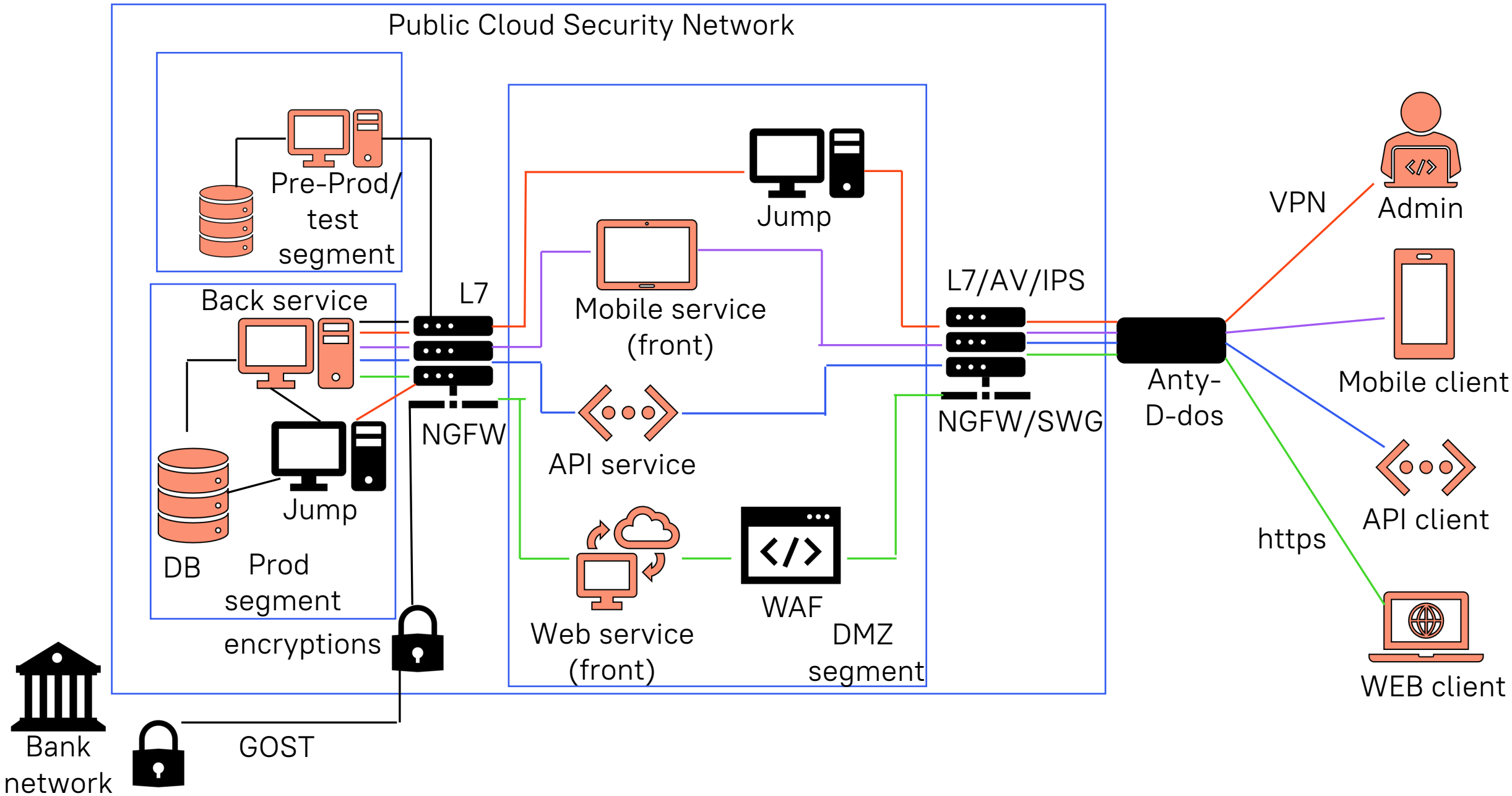


4. Безопасности облачных сред

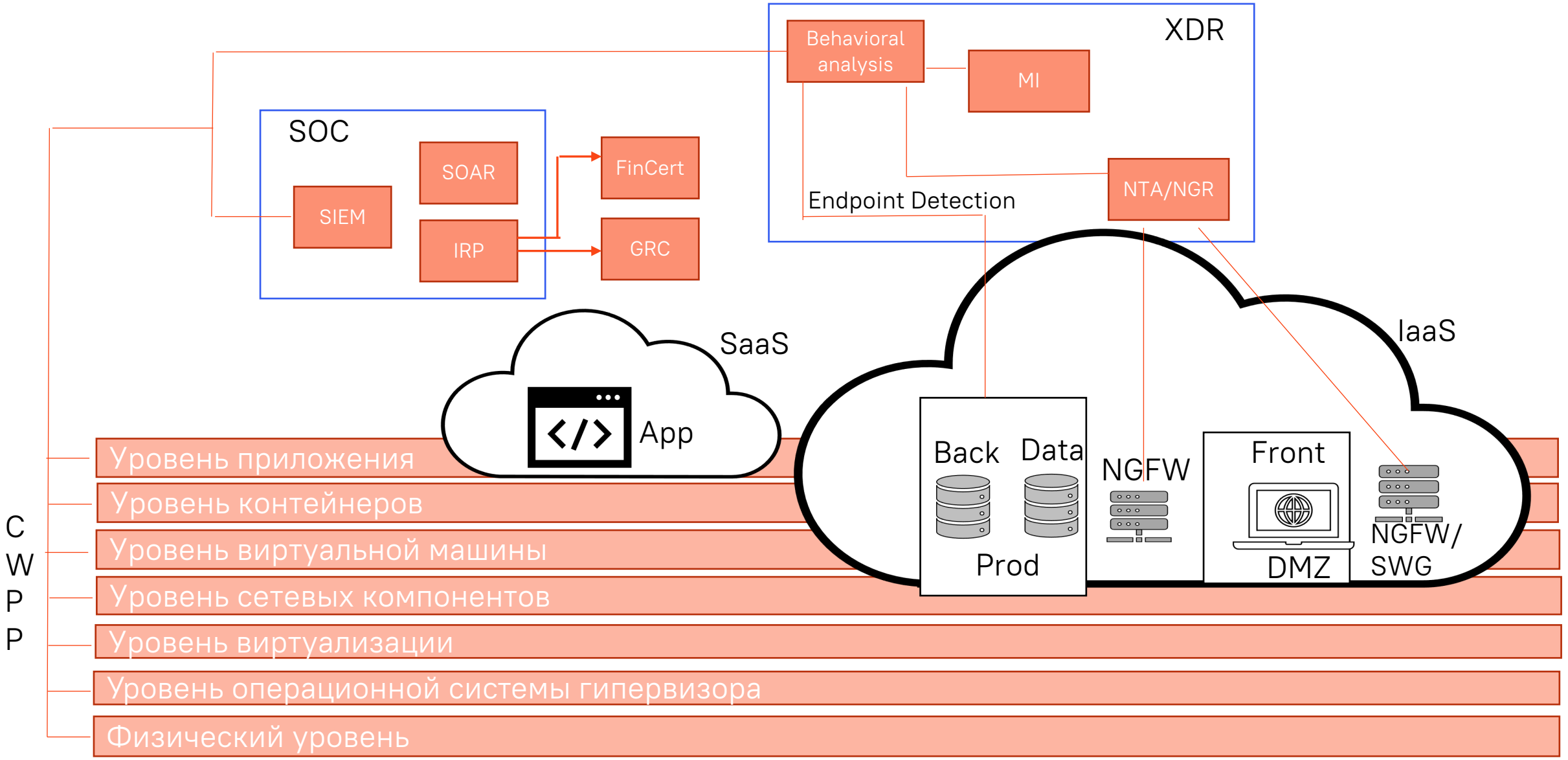
Управление доступом к данным в облаке



Безопасность сети и технологии пограничного доступа



Управление инцидентами в облачных средах



Спасибо

Ложкин Р.В.

E-mail: r.lozhkin@absolutbank.ru

АБСОЛЮТ БАНК