

# Анализ внешней среды

## Профиль

ФИО: Мустафаева Полина Махировна

Группа: ИДБ-22-06

Уровень: Бакалавр

## Сегмент

Кибербезопасность

## PESTEL

### P – Политические

- Усиление требований по защите критической инфраструктуры (КИИ)
- Расширение перечня обязательных мер по ИБ на уровне государства
- Господдержка отечественного ПО и импортозамещения
- Проверки регуляторов (ФСТЭК, ФСБ, ЦБ) становятся регулярными

### E – Экономические

- Увеличение расходов компаний на ИБ из-за роста числа инцидентов
- Колебание курса валют влияет на стоимость зарубежных решений
- Дефицит ИБ-специалистов повышает стоимость услуг
- Переход компаний на отечественные продукты для снижения ТСО

### S – Социальные

- Повышение цифровой грамотности сотрудников, но сохранение человеческого фактора
- Рост количества пользователей онлайн-сервисов увеличивает потребность в защите данных
- Популяризация удалённой работы усиливает требования к безопасности

### T – Технологические

- Массовое внедрение AI/ML в обнаружение угроз и аномалий
- Развитие облачных технологий и защищённых облаков
- Усложнение кибератак (APT, фишинг, социальная инженерия)

### E – Экологические

- Оптимизация энергопотребления дата-центров SOC и систем мониторинга.
- Использование энергоэффективного оборудования для инфраструктуры ИБ
- Экологические стандарты крупных заказчиков могут влиять на выбор поставщиков

### L – Правовые

- Обязательное соответствие ФЗ-152 (персональные данные)
- Требования регуляторов: ФСТЭК, ФСБ, ГОСТ/РД по ИБ
- Сертификация криптографии и ПО по ИБ
- Ужесточение ответственности за утечки и инциденты

# Анализ внешней среды

## Факторы и веса

Фактор	Вес
Соответствие ФЗ-187	0,22
SOC/SIEM-мониторинг 24/7	0,22
Anti-DDoS и веб-защита	0,18
Реагирование на инциденты (IR/SLA)	0,13
Аудит и тесты на проникновение	0,13
Интеграция с отечественными средствами ИБ	0,12

## Оценка компаний

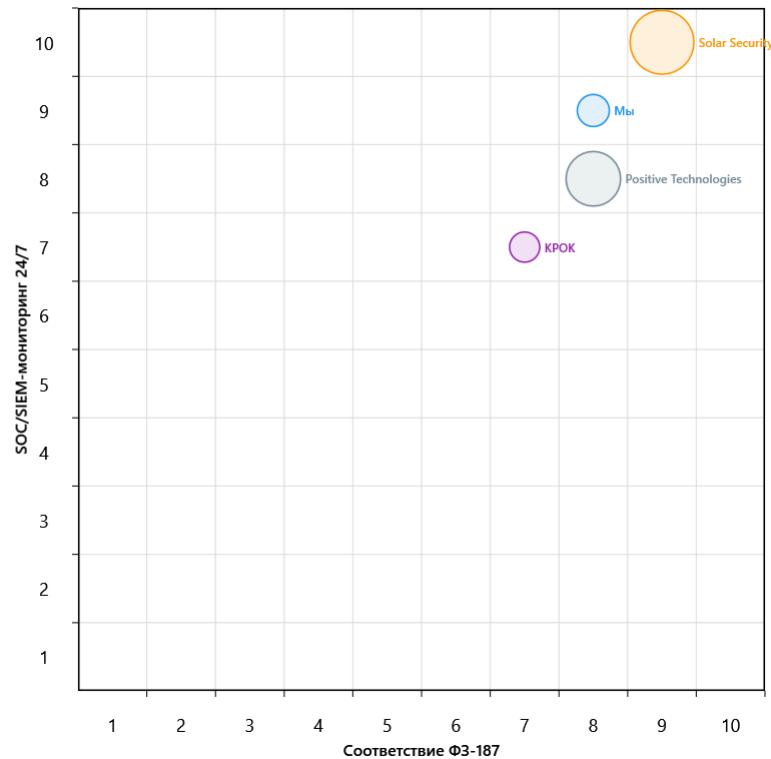
Фактор	Мы	Solar Security	Positive Technologies	KROK
Соответствие ФЗ-187	8	9	8	7
SOC/SIEM-мониторинг 24/7	9	10	8	7
Anti-DDoS и веб-защита	7	9	8	6
Реагирование на инциденты (IR/SLA)	8	10	8	6
Аудит и тесты на проникновение	8	8	10	7
Интеграция с отечественными средствами ИБ	9	8	9	7

## Сводка по компаниям

Компания	Доля рынка	Взвеш. рейтинг (0-10)
Мы	18,0 %	8,16
Solar Security	35,0 %	9,10
Positive Technologies	30,0 %	8,38
KROK	17,0 %	6,69

# Анализ внешней среды

## Стратегическая карта 1



### Пояснение

X: Соответствие ФЗ-187

Y: SOC/SIEM-мониторинг 24/7

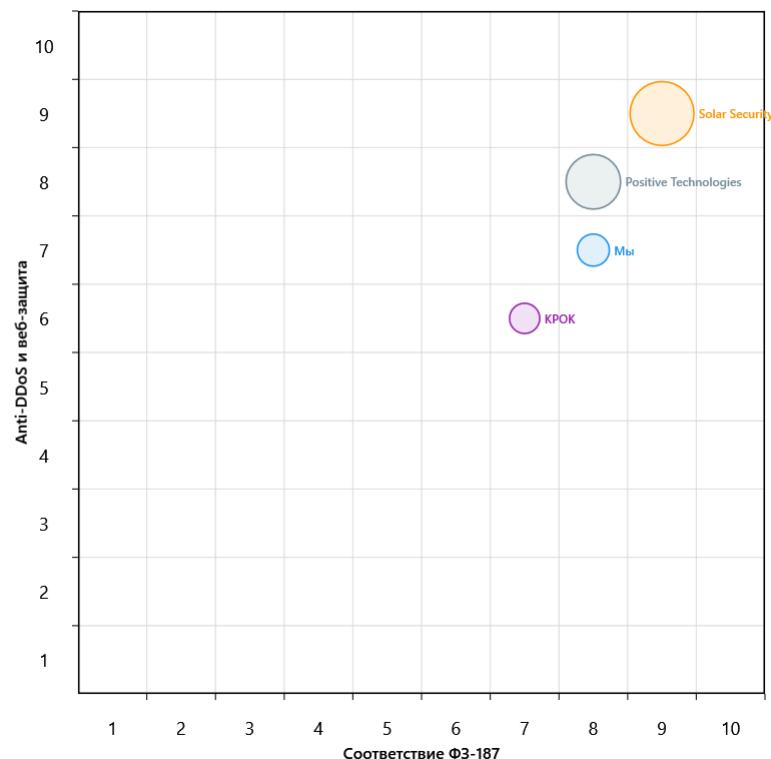
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Развитие комплексного соответствия законодательству с круглосуточным мониторингом угроз

# Анализ внешней среды

## Стратегическая карта 2



### Пояснение

X: Соответствие ФЗ-187

Y: Anti-DDoS и веб-защита

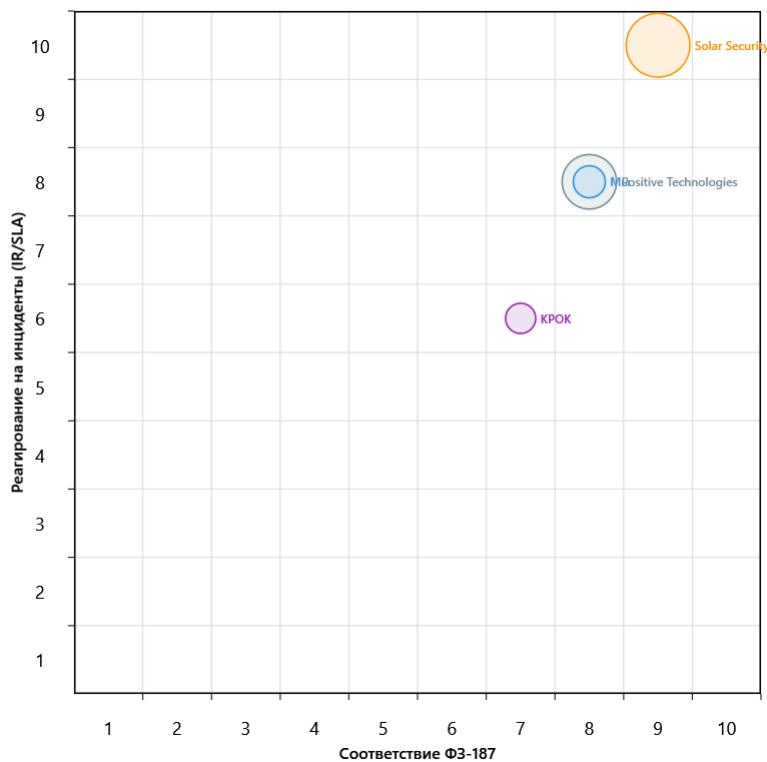
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Усиление нормативного соответствия через защиту веб-приложений и предотвращение DDoS-атак

# Анализ внешней среды

## Стратегическая карта 3



### Пояснение

X: Соответствие ФЗ-187

Y: Реагирование на инциденты (IR/SLA)

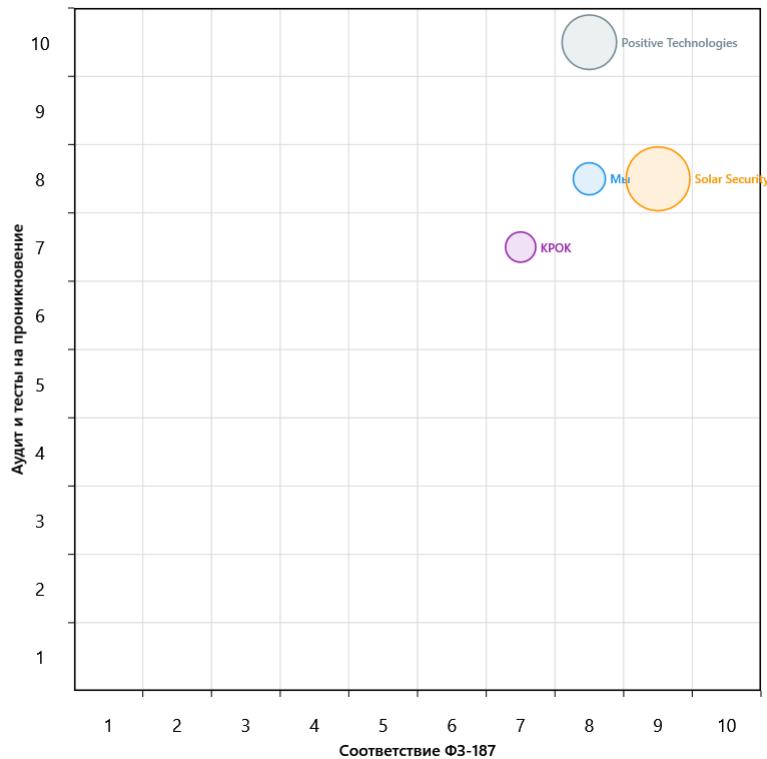
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Внедрение регламентированных процедур реагирования на инциденты с соблюдением требований ФЗ-187

# Анализ внешней среды

## Стратегическая карта 4



### Пояснение

X: Соответствие ФЗ-187

Y: Аудит и тесты на проникновение

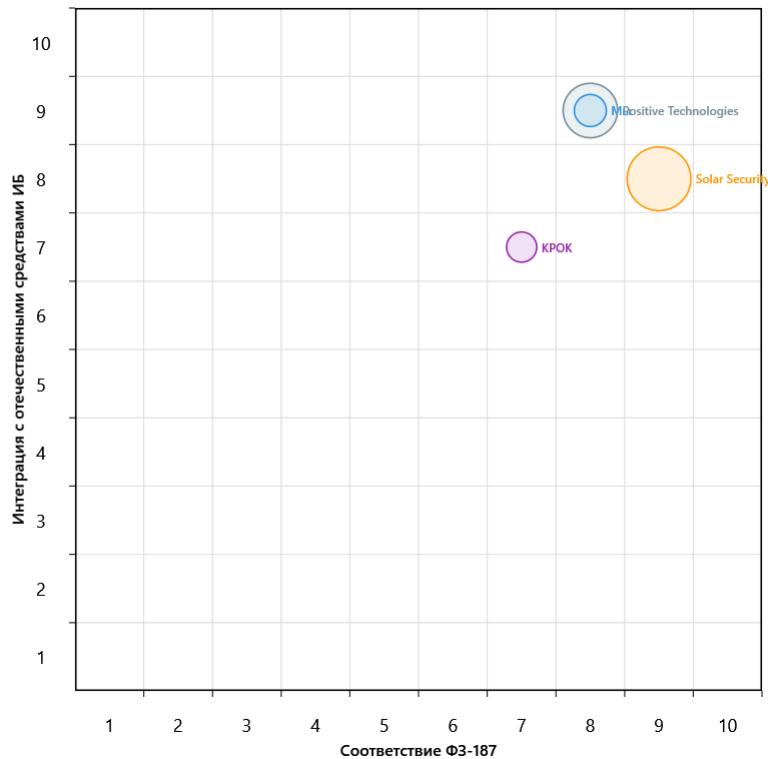
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Совмещение соответствия ФЗ с регулярной проверкой защищенности инфраструктуры

# Анализ внешней среды

## Стратегическая карта 5



### Пояснение

X: Соответствие ФЗ-187

Y: Интеграция с отечественными средствами ИБ

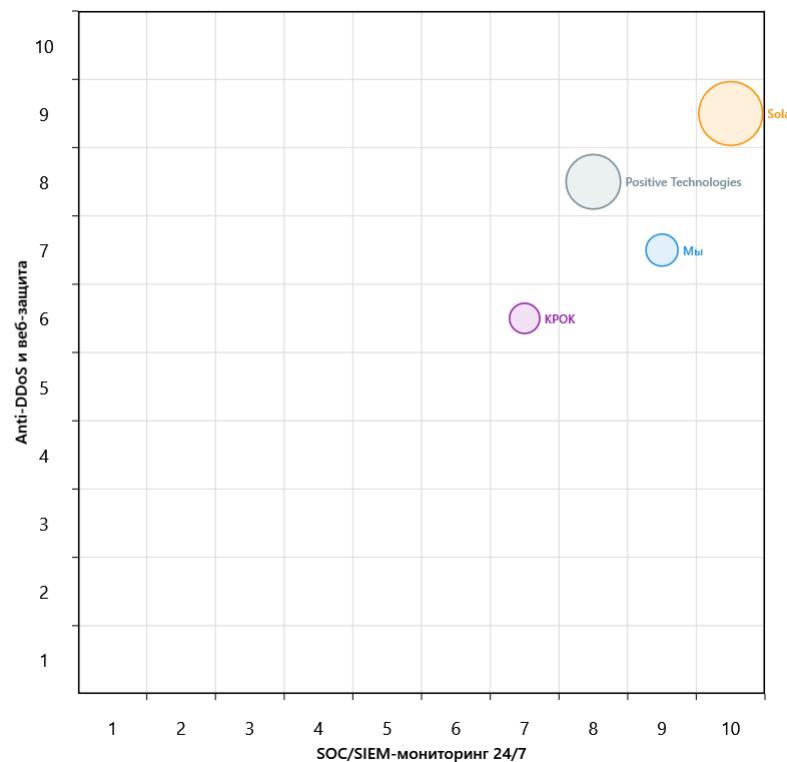
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Развитие соответствия ФЗ через использование отечественных решений по ИБ

# Анализ внешней среды

## Стратегическая карта 6



### Пояснение

X: SOC/SIEM-мониторинг 24/7

Y: Anti-DDoS и веб-защита

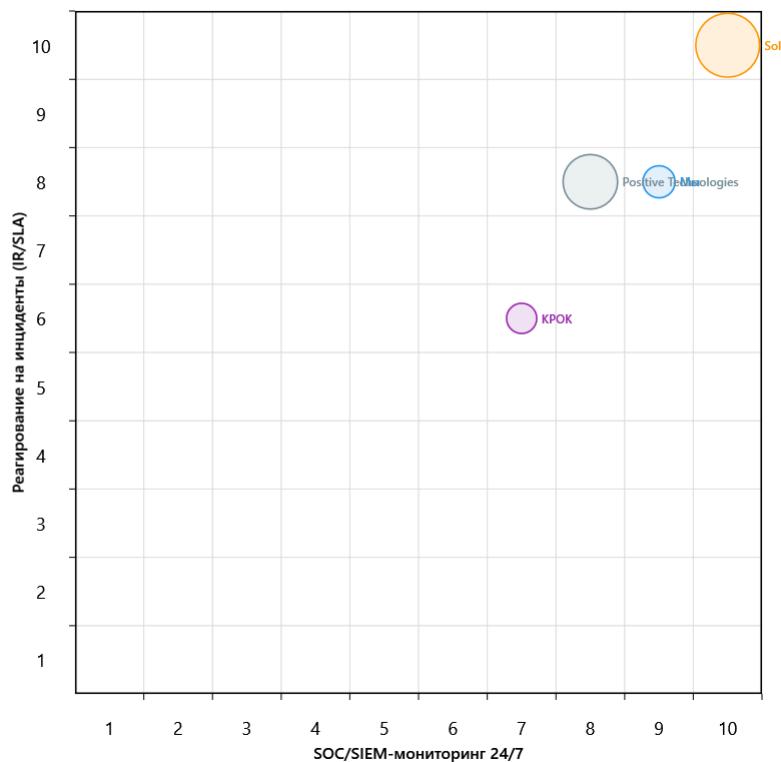
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Интеграция постоянного мониторинга с проактивной защитой от веб-угроз и DDoS-атак

# Анализ внешней среды

## Стратегическая карта 7



### Пояснение

X: SOC/SIEM-мониторинг 24/7

Y: Реагирование на инциденты (IR/SLA)

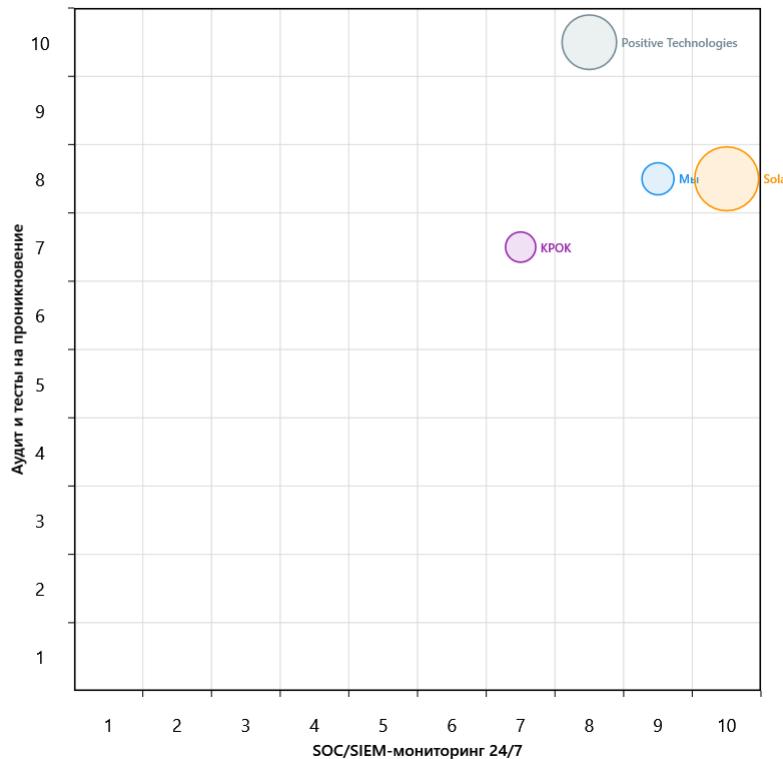
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Объединение мониторинга и оперативного реагирования на инциденты для минимизации рисков

# Анализ внешней среды

## Стратегическая карта 8



### Пояснение

Х: SOC/SIEM-мониторинг 24/7

Y: Аудит и тесты на проникновение

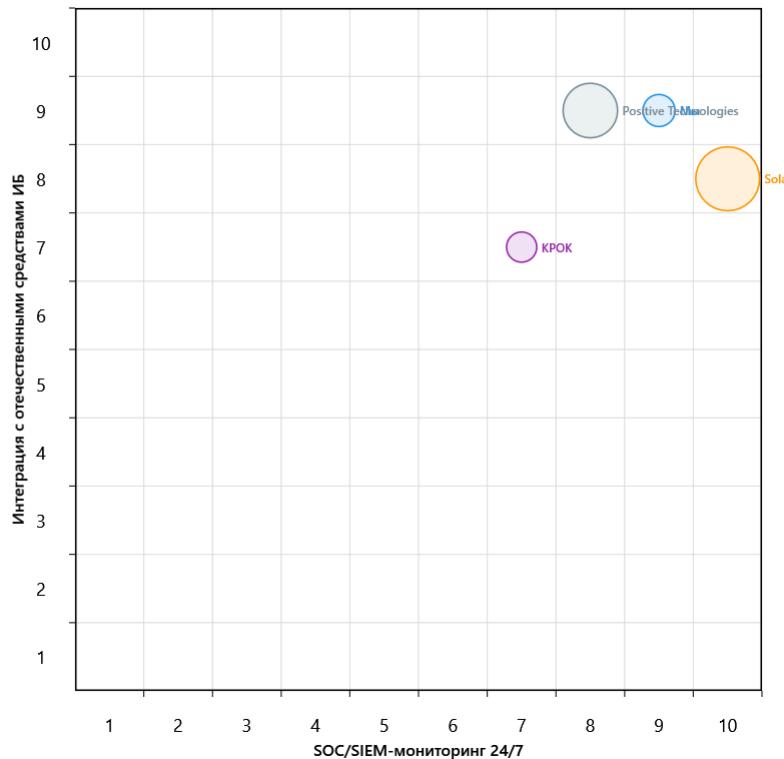
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Использование мониторинга для приоритизации и оценки результатов аудита

# Анализ внешней среды

## Стратегическая карта 9



### Пояснение

X: SOC/SIEM-мониторинг 24/7

Y: Интеграция с отечественными средствами ИБ

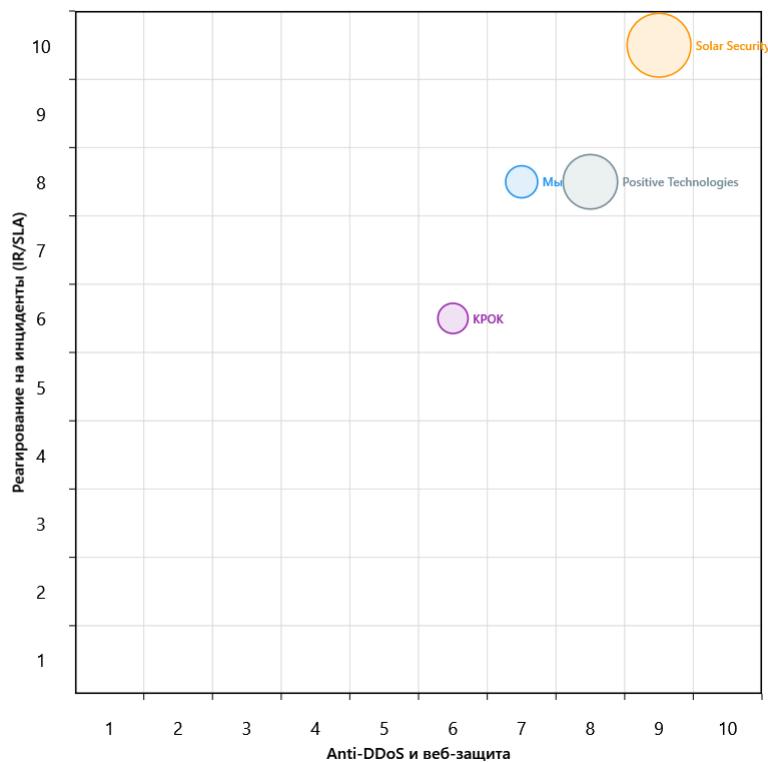
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Развитие локальных решений мониторинга и аналитики угроз

# Анализ внешней среды

## Стратегическая карта 10



### Пояснение

X: Anti-DDoS и веб-защита

Y: Реагирование на инциденты (IR/SLA)

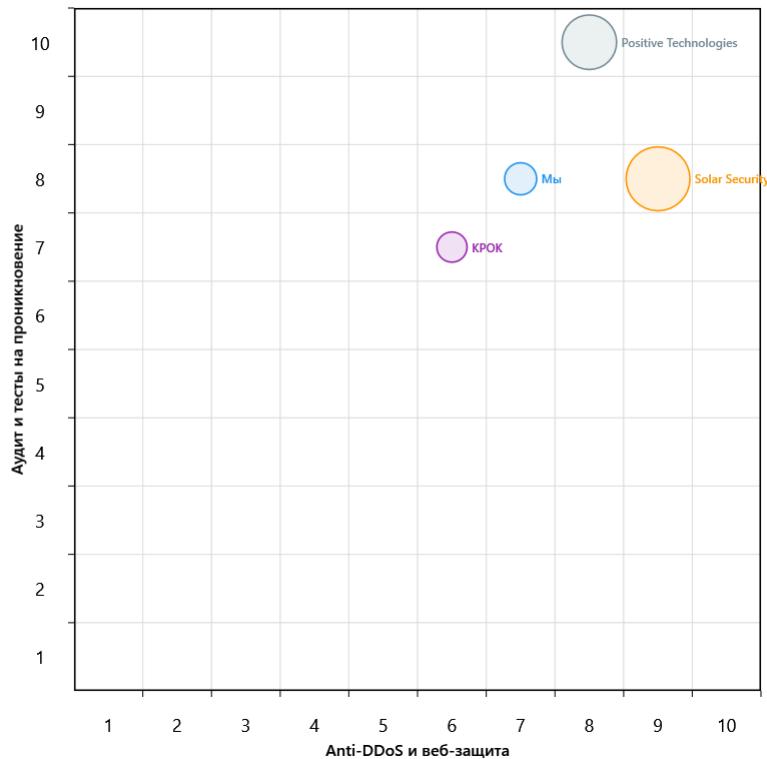
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Усиление защиты веб-сервисов через автоматическое и ручное реагирование на атаки

# Анализ внешней среды

## Стратегическая карта 11



### Пояснение

X: Anti-DDoS и веб-защита

Y: Аудит и тесты на проникновение

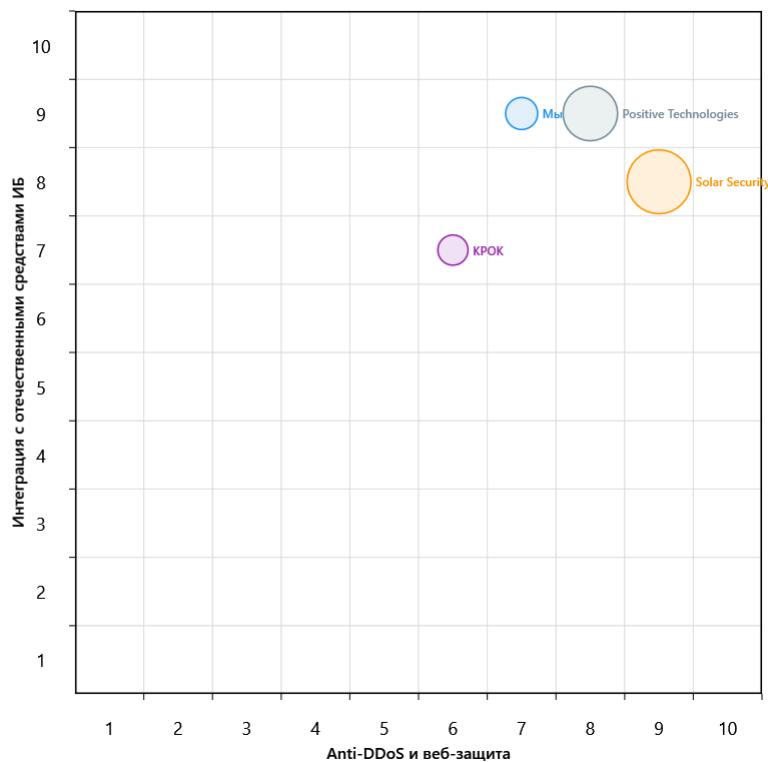
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Повышение эффективности защиты через регулярное тестирование уязвимостей

# Анализ внешней среды

## Стратегическая карта 12



### Пояснение

X: Anti-DDoS и веб-защита

Y: Интеграция с отечественными средствами ИБ

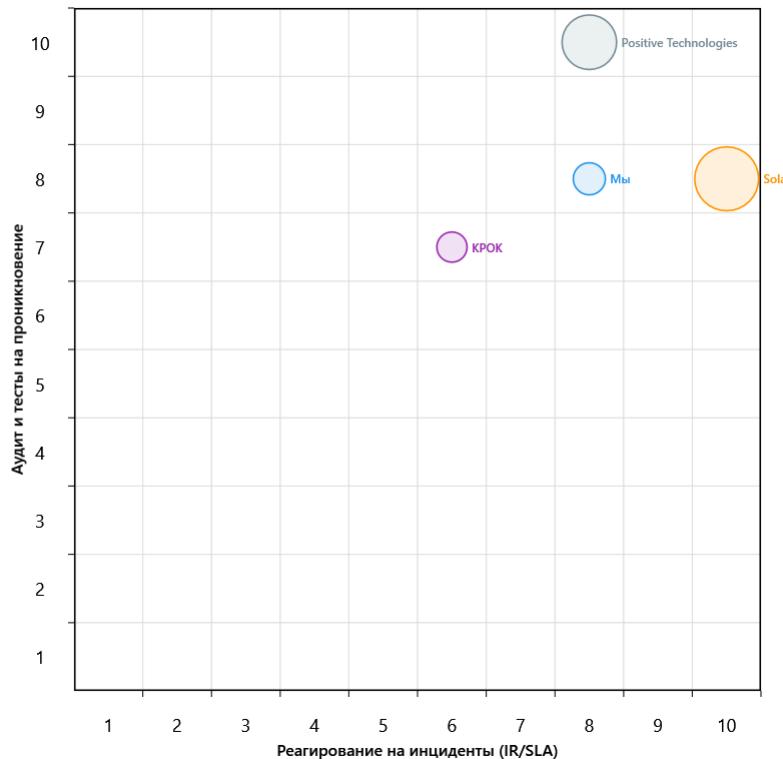
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Развитие защиты веб-приложений с использованием локальных технологий ИБ

# Анализ внешней среды

## Стратегическая карта 13



### Пояснение

X: Реагирование на инциденты (IR/SLA)

Y: Аудит и тесты на проникновение

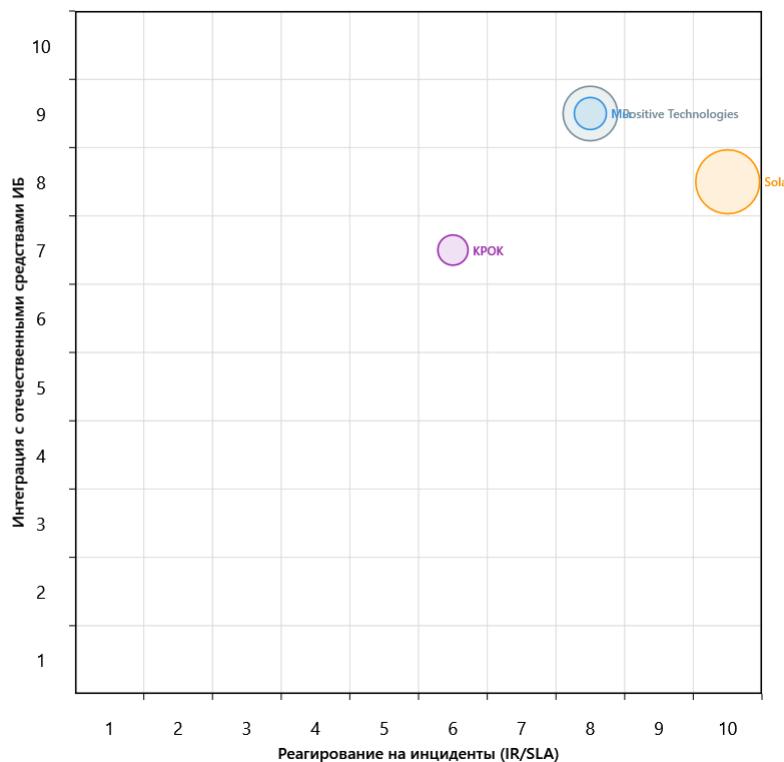
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Оптимизация процессов реагирования на основе данных аудита

# Анализ внешней среды

## Стратегическая карта 14



### Пояснение

Х: Реагирование на инциденты (IR/SLA)

Y: Интеграция с отечественными средствами ИБ

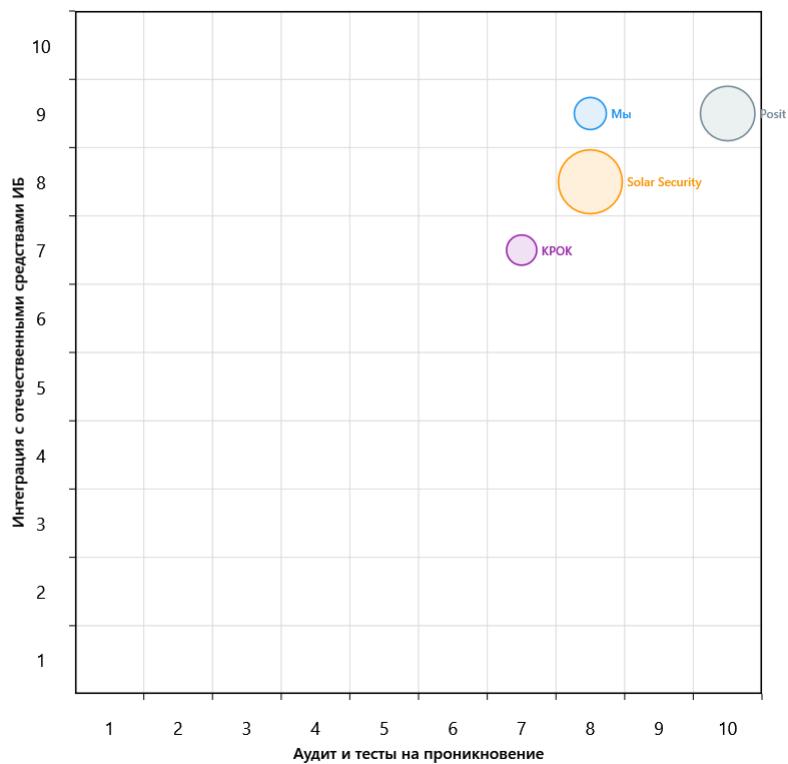
Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Совершенствование процессов реагирования через внедрение отечественных решений ИБ

# Анализ внешней среды

## Стратегическая карта 15



### Пояснение

X: Аудит и тесты на проникновение

Y: Интеграция с отечественными средствами ИБ

Подсказка: отметьте лидеров по осям и зоны роста.

### Направление развития

Повышение качества проверки защищенности с помощью локальных инструментов

# Анализ внешней среды

## Итоги по компаниям

### Итоги

В сегменте кибербезопасности лидером по большинству направлений развития выступает Solar Security. Они демонстрируют стабильность и зрелость в ключевых областях, включая соответствие ФЗ-187, SOC/SIEM-мониторинг и защиту веб-приложений. Positive Technologies и наша компания показывают сильные позиции по отдельным направлениям, особенно в интеграции с отечественными решениями и автоматизации реагирования на инциденты, что отражено в рейтингах «Positive Technologies» и «Мы» по оси Y. Основные точки роста для участников рынка - расширение интеграции с российскими средствами информационной безопасности, повышение автоматизации реагирования на инциденты, а также активное использование аудита и тестов на проникновение для повышения эффективности защиты.

Компания	Доля рынка	Взвешенный рейтинг (0-10)
Мы	18,0 %	8,16
Solar Security	35,0 %	9,10
Positive Technologies	30,0 %	8,38
КРОК	17,0 %	6,69

Лидер по рейтингу: Solar Security (9,10).