



Аутсорсинг ИБ в облако

Рынок, тенденции и проблемы

Николай Носов
обозреватель-эксперт ИКС-Медиа



История цивилизации — история развития аутсорсинга.



1. Процессы цифровизации и цифровой трансформации, требующие больше компьютеров и соответственно средств их защиты.

Из новых, только набирающих силу:

- введение цифровых валют и как следствие развитие защищающих их продуктов;
- бурное развитие ИИ и как следствие рост рынка средств защиты от атак с использованием ИИ и атак на процессы обучения ИИ;
- переход на постквантовую криптографию.

2. Рост геополитической турбулентности в мире приводит к росту числа кибератак, причем к традиционным атакам хакеров с целью получения финансовой выгоды все больше добавляется кибертерроризм с целью воздействия на лидеров, экономику и население атакуемой страны. Растет число атак на промышленность (АСУ ТП), сложность и массовость атак.

3. Увеличивающаяся простота проведения кибератак, обеспечиваемая повышением компьютерной грамотности, прогрессом в системах автоматизации (автоматические сканеры уязвимостей, использование ИИ), специализацией и разделением труда у хакеров (одни занимаются взломом, другие кражей, третьи — выводом средств)

1. Повышенный по сравнению с общемировым уровень атак.
2. Повышенный уровень атак, связанных с кибертерроризмом, что заставляет заниматься вопросами киберзащиты сектор СМБ, не так привлекательный с точки зрения «финансовых» хакеров.
2. Тренд на импортозамещение, связанный с уходом иностранных вендоров, потерей к ним доверия и давлением регуляторов.



1. Высокая ставка рефинансирования, ограничивающая инвестиции в разработку и внедрение средств киберзащиты
2. Нехватка кадров.
3. Санкции, особенно чувствительные для использования аппаратных средств защиты



MSSP (Managed Security Service Provider) — это провайдер, который предлагает управляемые услуги безопасности, используя свои ресурсы и экспертизу.

- Мониторинг безопасности 24/7 (SOC)
- Управление сетевыми устройствами (брандмауэры, IPS/IDS)
- Анализ и расследование инцидентов.



MDR (Managed Detection and Response) - MDR предполагает более активное участие в расследовании и устранении угроз, в то время как MSSP может ограничиваться мониторингом и уведомлениями.

MDR специализируется на анализе угроз, расследовании и реагировании на инциденты, часто с использованием современных технологий, таких как искусственный интеллект и машинное обучение..



SECaaS — облачная модель предоставления услуг безопасности, где провайдер предлагает клиенту доступ к инструментам и платформам безопасности через облако. Клиент использует эти инструменты, но управление и настройка могут оставаться на его стороне.

Примеры:

- Облачный антивирус.
- Защита от DDoS-атак.
- Управление идентификацией и доступом (IAM).
- Шифрование данных в облаке

ТОП 30 MSSP			
Позиция	Мировой провайдеры MSSP	Страна/Штаб-квартира	Выручка 2023, € млн
1	Thales	Франция	2400
2	Orange Cyberdefense	Франция	1100
3	Telefónica Tech Inc.	США	751
4	Rapid7	США	719
5	ECS Tech	США	693
6	Optiv	США	664
7	Ensign InfoSecurity	Сингапур	292
8	Dbappsecurity Co.,Ltd	Китай	284
9	eSentire	Канада	146
10	sirar by stc	Саудовская Аравия	145
11	Kudelski Security	Швейцария	110
12	mnemonic	Норвегия	103
13	ISH Tecnologia	Бразилия	87
14	DYOPATH	США	79
15	Solar	Россия	75

Первым провайдером MSS (Managed Security Services) стала американская компания US West, которая еще в 1997 г. начала предлагать клиентам использовать ей принадлежащий и ею управляемый файрвол – Check Point Firewall-1.



Сложность киберугроз

Нехватка квалифицированных кадров

Деньги

Регуляторика

Гибкость и масштабируемость

Доступ к передовым технологиям

Быстрое реагирование

Снижение нагрузки на ИТ



Недоверие клиентов

Сложность решений

Стоимость решений

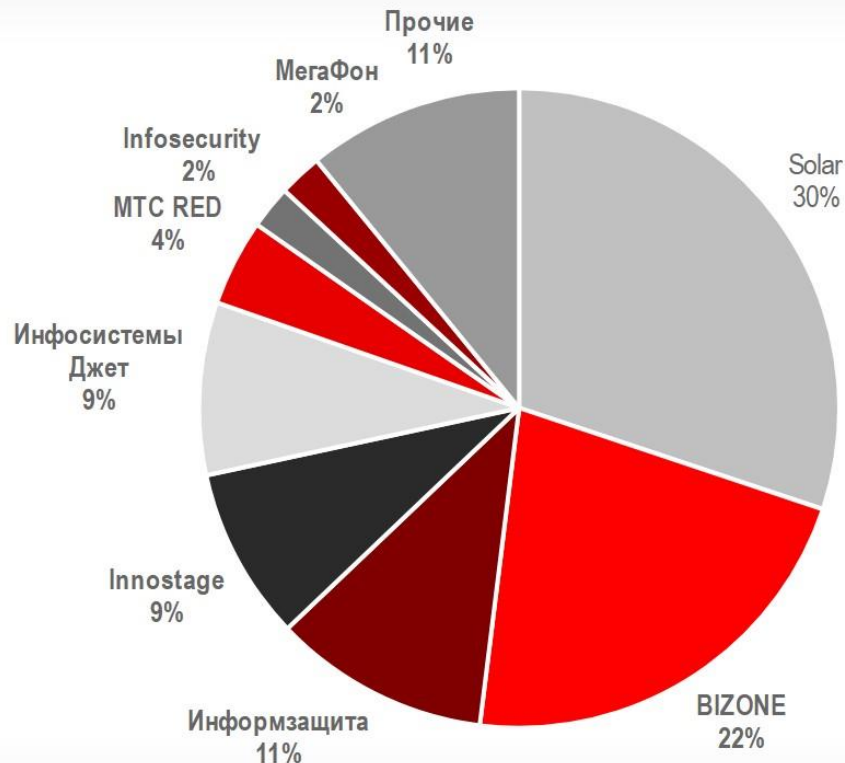
**Сложности
интеграции**

Кадры

Структура рынка SOC по игрокам



Доли игроков рынка в 2023 году в выручке, %



Источник: оценки iKS-Consulting, данные компаний

По оценке, iKS-Consulting российский рынок SOC по итогам 2023 года составил порядка 25,4 млрд руб

Рынок в основном формируют специализированные игроки рынка кибербезопасности, но также активно развивают это направление и телеком-операторы, которые пока в начале пути

Источник: оценки iKS-Consulting, данные компаний





Рост спроса на SOC и удаленную эксплуатацию

Развитие облачных сервисов безопасности

ИИ

DLP

Интеграция с ИТ

1 Функционал

2 Бренд

3 Внедрения

4 Поддержка

5 Разработка

6 Договор

7 Независимая
оценка





Николай Носов
эксперт-обозреватель iKS-Media
nikolay.nosov@iksmedia.ru