

Актуальные тренды в области ИБ

Вячеслав Максимов
технический директор, «Информзащита»

кибербезопасность
в эпоху перемен

6 КЛЮЧЕВЫХ ВЫЗОВОВ

кибербезопасность
в эпоху перемен



Распространение ML/AI



Рост киберугроз



Атаки на цепочки поставок



Требования регуляторов



Дефицит ресурсов



Импортозамещение

#1: Лавинное распространение ML/AI

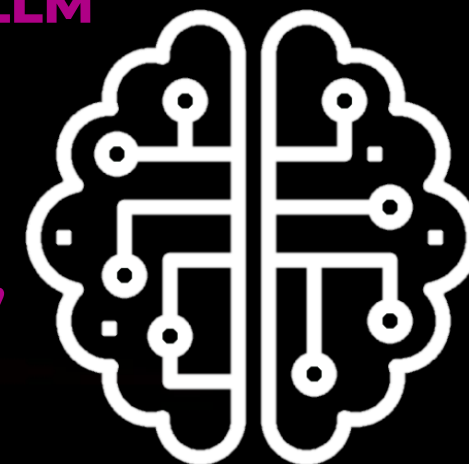
кибербезопасность
в эпоху перемен



Рост доступности и распространения технологий GenAI / LLM

- › Удобны в использовании, облегчают работу
- › Являются не только помощниками в работе, но и каналами утечки данных
- › Широко применяются злоумышленниками
- › ...

ML – не просто новая технология, а изменение парадигмы, требующее немедленной реакции со стороны ИБ



Решения: формирование доверенных цифровых помощников, MLSecOps, развитие культуры кибербезопасности

#2: Рост киберугроз

кибербезопасность
в эпоху перемен



Усиление киберпреступности

- › Распространение и доступность ВПО
- › Рост организации киберпреступлений (специализация, конвейеризация, автоматизация)
- › Расширение применения технологий ML/AI в киберпреступности
- › Развитие и распространение модели Cybercrime-as-a-Service
- › Кибервойны

Рост количества киберпреступлений

- › 40% их всех преступлений в 2024 году пришлось на кибермошенничество
- › Рост количества и объема утечек данных
- › Рост количества громких инцидентов, связанных с реализацией киберугроз

Работа с киберугрозами сегодня – не про риски, а про быстрое выявление и реагирование

Решения: SOC, киберучения, рабочие DRP и BCP, управление уязвимостями (VM, pentest, DevSecOps)



#3: Атаки на цепочки поставок

кибербезопасность
в эпоху перемен



Атака через компрометацию доверенных поставщиков

- › Вендоры «коробочного» программного обеспечения
- › Разработчики заказного ПО
- › Используемые пакеты Open Source
- › ИТ и ИБ интеграторы
- › Облачные сервис-провайдеры
- › Поставщики MSSP-сервисов
- › ...



Постоянный рост количества атак на поставщиков услуг и решений

Решения: PUM/PAM, SCA/OSA, ZeroTrust, программы контроля безопасности поставщиков

#4: Изменение требований регуляторов

кибербезопасность
в эпоху перемен



Развитие подходов к защите ПДн

- › уголовная ответственность за неправомерную обработку ПДн
- › рост штрафов для ФЛ и ЮЛ за нарушения и утечки, оборотные штрафы за повторные утечки
- › ужесточение требований по локализации БД с ПДн
- › требования и методы по обезличиванию ПДн

Развитие подходов по защите КИИ

- › перечни типовых ОКИИ по отраслям, отраслевые особенности категорирования ОКИИ
- › требования о проведении инвентаризации ОКИИ и пересмотре бюджетов на импортозамещение
- › требования к Субъектам КИИ о непрерывном взаимодействии с ГосСОПКА



Планомерная работа ВСЕХ регуляторов по развитию нормативной базы, с учетом актуальных рисков для отрасли

Решения: Планомерная работа по поддержанию соответствия, внутренние и внешние аудиты, консалтинг, SGRC

#5: Дефицит ресурсов

кибербезопасность
в эпоху перемен

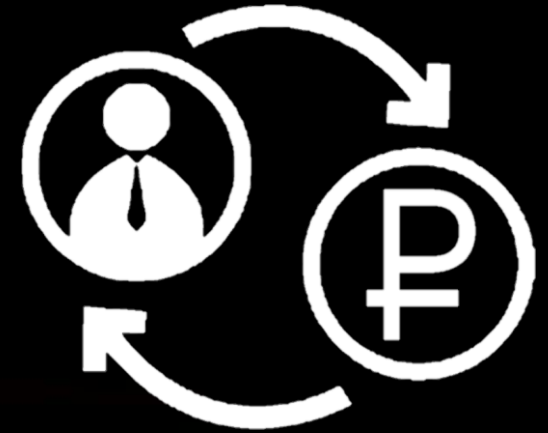


Жесткое ограничение финансовых ресурсов

- › Высокая ключевая ставка
- › Рост совокупной стоимости владения (в том числе для ИТ и ИБ)
- › Ужесточение ограничения бюджетов

Кадровый голод в сфере ИБ

- › Взрывной рост востребованности специалистов по ИБ
- › Демографическая яма 90-х
- › Жесткая конкуренция работодателей за любых ИБ-специалистов, вне зависимости от уровня компетенций



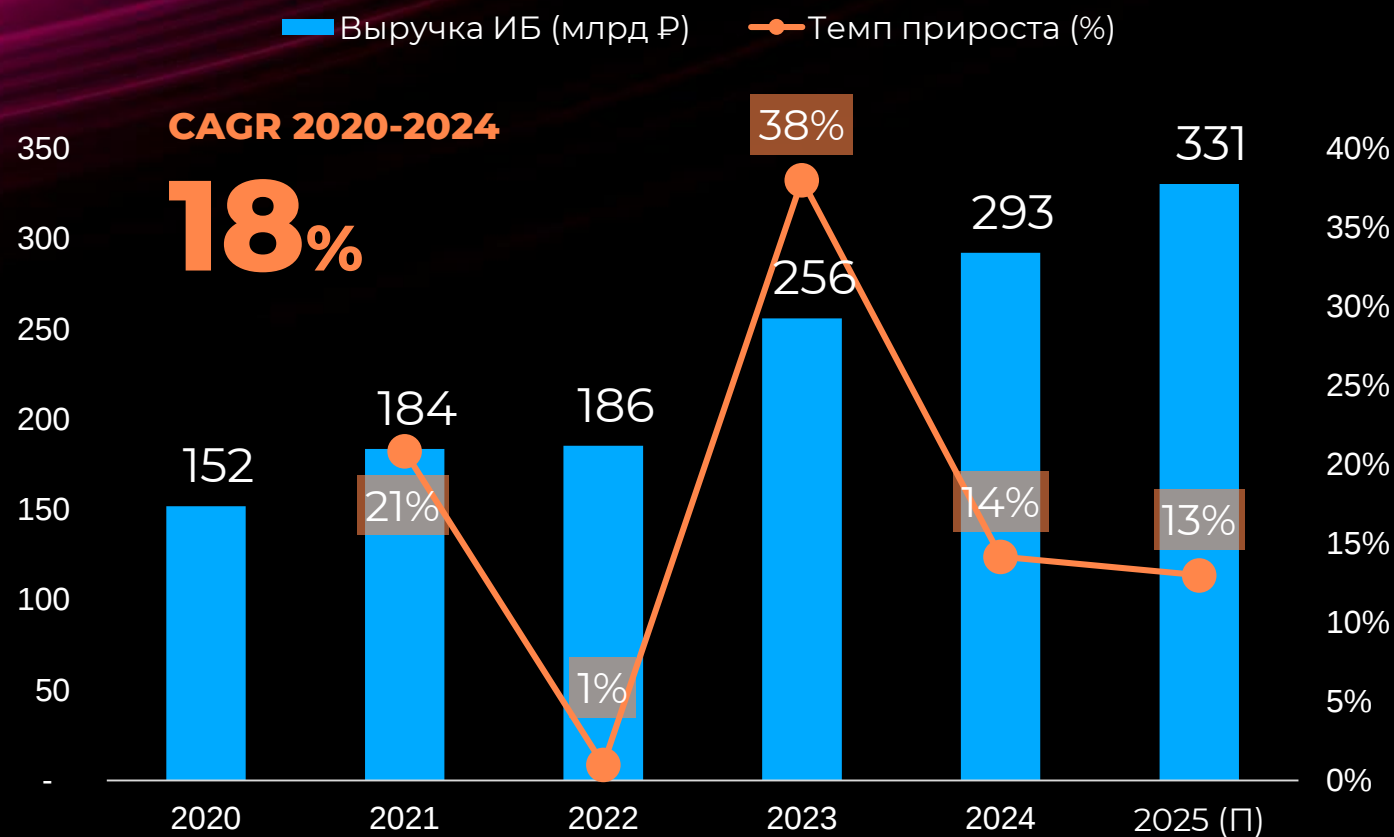
Решения: Аутсорсинг и MSS-решения в области ИБ

Динамика рынка ИБ

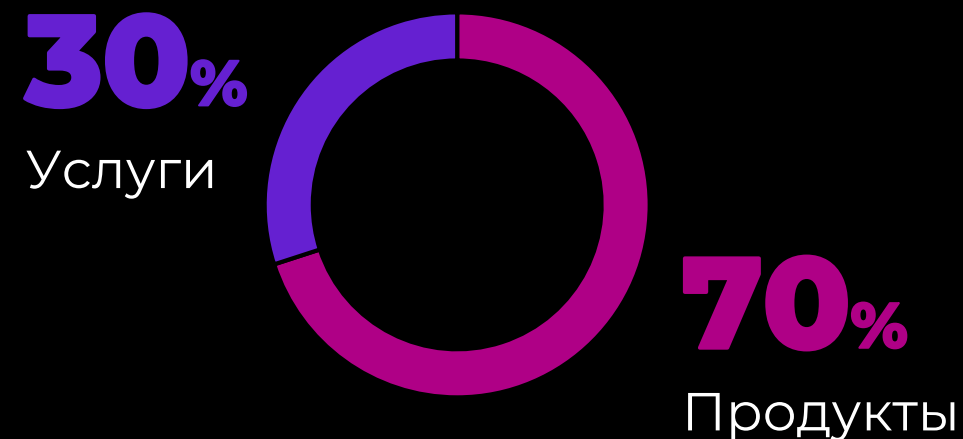
кибербезопасность
в эпоху перемен

Объем рынка ИБ

кибербезопасность
в эпоху перемен



По аналитическим данным Информзащиты



✓ Долевое соотношение продуктов и услуг практически не меняется по годам

Динамика - Продукты

кибербезопасность
в эпоху перемен



Темпы роста



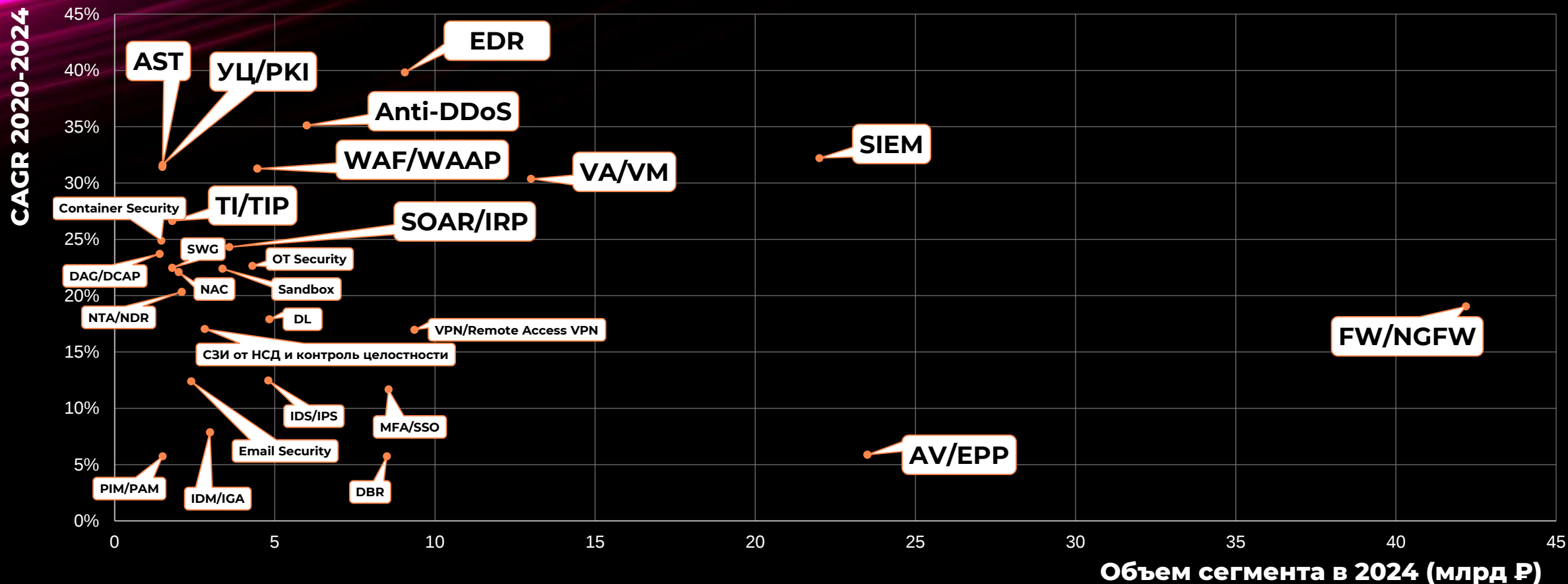
Долевое распределение



По аналитическим данным Информзащиты

Структура рынка ИБ – Продукты

кибербезопасность
в эпоху перемен



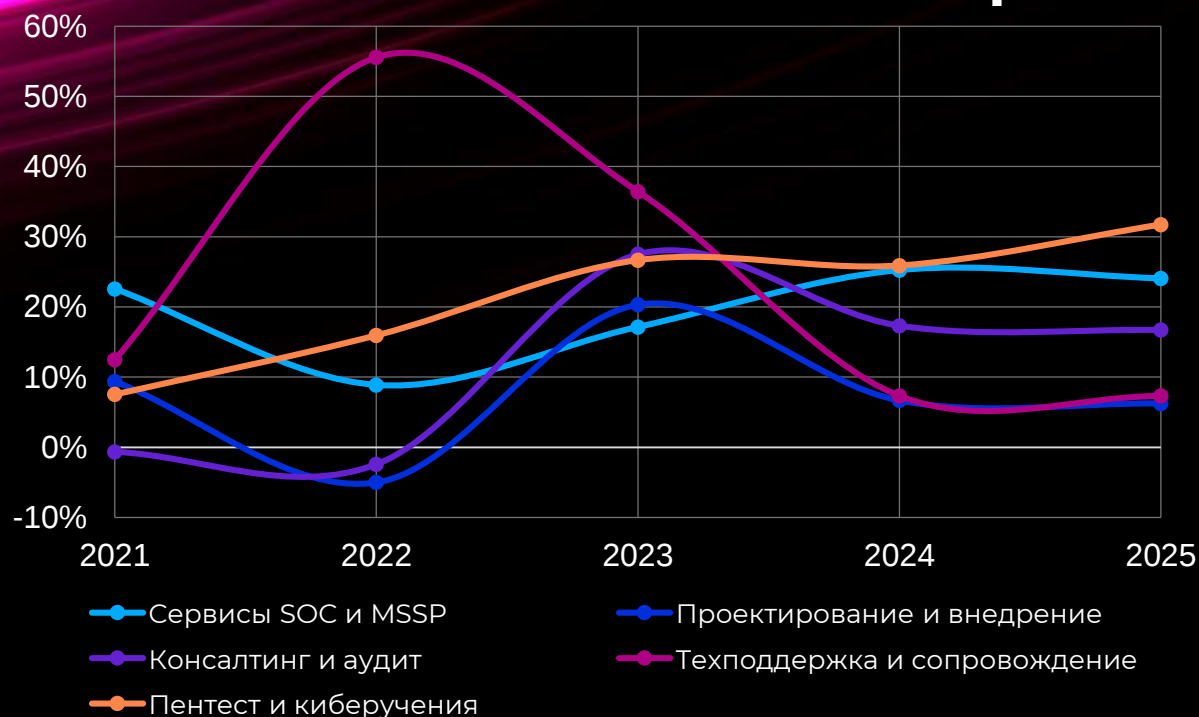
По аналитическим данным Информзащиты

Динамика - Услуги

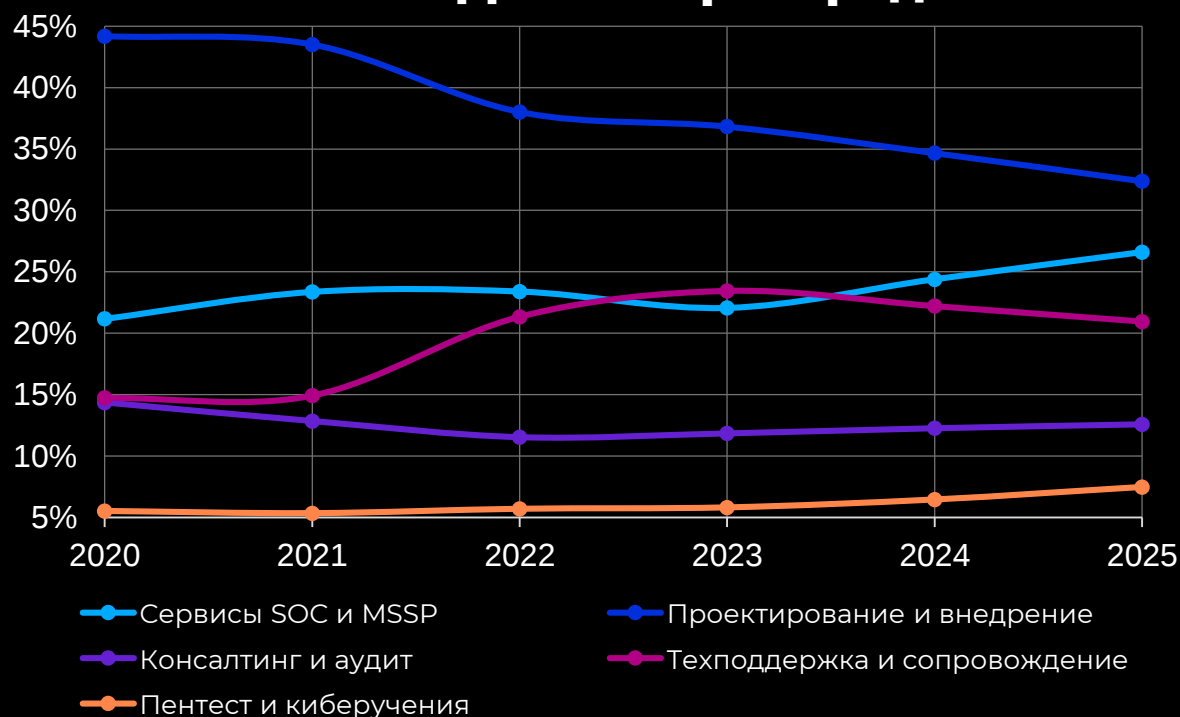
кибербезопасность
в эпоху перемен



Темпы роста

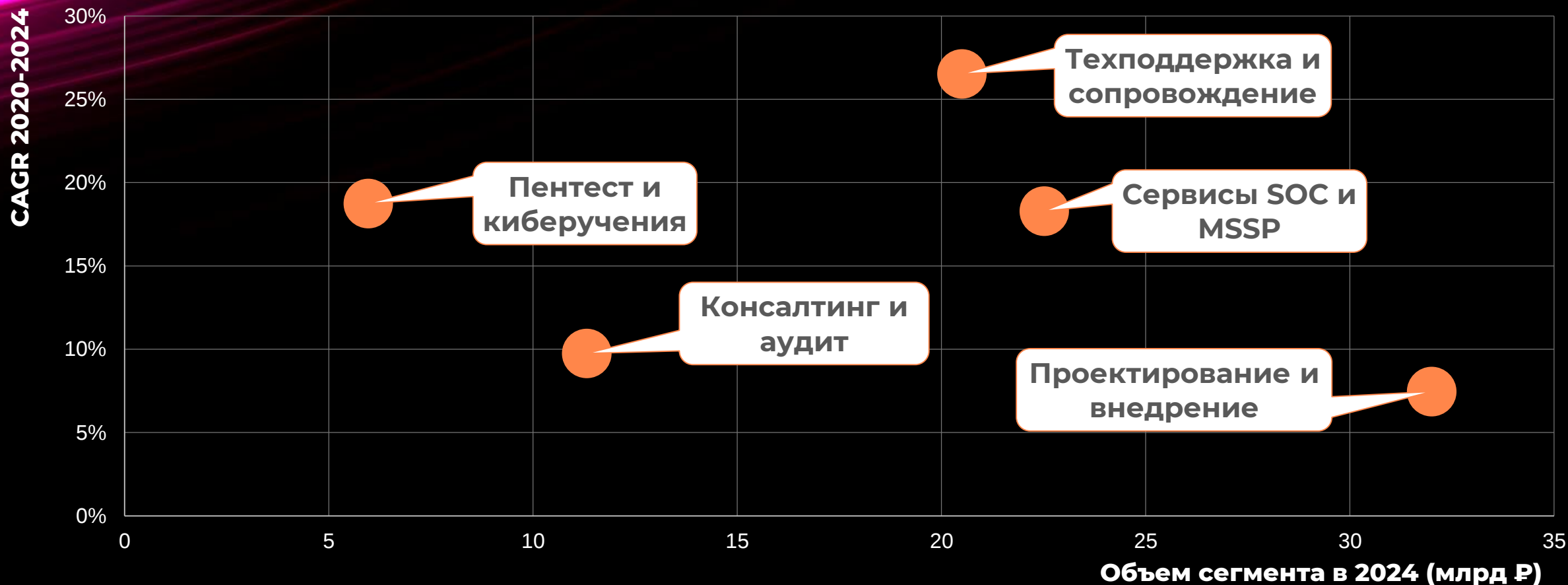


Долевое распределение



Структура рынка ИБ – Услуги

кибербезопасность
в эпоху перемен



По аналитическим данным Информзащиты

Драйверы и барьеры

кибербезопасность
в эпоху перемен



Драйверы роста рынка ИБ

- ↑ Импортозамещение
- ↑ Изменения требований регуляторов
- ↑ Рост числа кибератак
- ↑ Усиление кооперации между службами ИТ и ИБ

Барьеры роста рынка ИБ

- ↓ Высокая ключевая ставка
- ↓ Сокращение бюджетов ИТ и ЦТ
- ↓ Кадровый голод
- ↓ Снижение эффективности бизнеса при переходе на отечественное ПО

Общие тренды рынка ИБ

- ✓ Концентрация рынка ИБ в руках крупнейших поставщиков продолжается
- ✓ Формирование вендорами полноценных экосистем из их продуктов

Точки роста

кибербезопасность
в эпоху перемен



✓ **Сервисы SOC, MSSP, экспертные сервисы**

✓ **NGFW:** Потенциал новых решений NGFW еще не реализован в полной мере

✓ Пока не реализован потенциал **решений для МСБ**

✓ Рост интереса к собственным разработкам и к аналогам иностранных решений. Одной из перспективных ниш остается **безопасная разработка**

✓ На рынке ИБ пока не хватает ряда классов технологий — **NAC, SD-WAN, SASE, решений для защиты сетей IoT**

✓ Имеют потенциал расширения рынка **технологии управления доступом:** решения классов IdM, PAM и DAG/DCAP, технологии защиты данных и противодействия утечкам

✓ Импортозамещение особенно актуально в следующих направлениях:

- **Кластерные МЭ уровня ядра сети** с общей пропускной способностью свыше 500 Гб/с
- **Системы защиты от DDoS-атак высокой интенсивности** с пропускной способностью от 1 Тб/с и выше.
- **Высокопроизводительные средства анализа исходного кода** под множество языков программирования с нативной интеграцией в конвейер DevSecOps
- **Горизонтально масштабируемые WAF-решения** для защиты веб-приложений от целевых атак при высоких нагрузках
- **Криптографические модули для защиты каналов связи** с производительностью не менее 50 Гб/с на устройство
- **SIEM-платформы для обработки больших и сверхбольших потоков событий**, охватывающие тысячи активов и обеспечивающие длительное хранение логов

Спасибо за внимание!

Вячеслав Максимов
технический директор, «Информзащита»

кибербезопасность
в эпоху перемен