информзащита

Критические точки кибербезопасности в контексте развития ИИ

Андрей Тимошенко
Директор по развитию

кибербезопасность
в эпоху перемен

Ключевые аспекты для стратегического прогнозирования в эпоху ИИ

информзащита

1. Критическая масса ИИ-агентов: $N > 10^8$
2. Порог плотности взаимодействия с ИИ: $\rho > 0.6$
3. Нейропсихологические и когнитивные трансформации
4. Неравномерный экономический рост и регулирование
5. Психо-социальная турбулентность

Ключевые аспекты влияния

информзащита

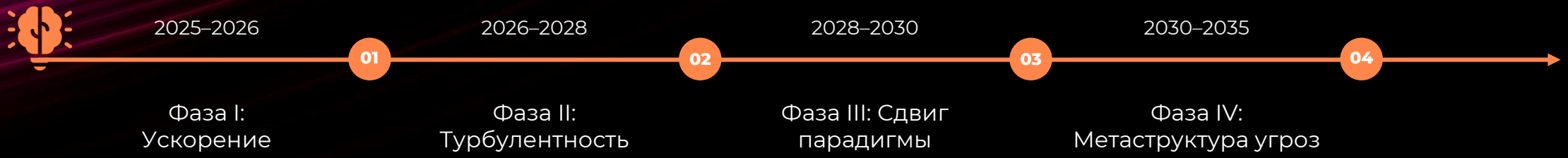
Критическая масса ИИ-агентов:
$N > 10^8$

Порог сетевой плотности:
$\rho > 0.6$

Системные эффекты

Эффект	Пример
Массовое изменение поведения	Студенты повсеместно используют ChatGPT – меняются способы обучения, падает критическое мышление
Информационные искажения	Генерация контента ИИ приводит к замещению оригинального контента «маркетинговыми лентами»
Кибербезопасность	ИИ-боты атакуют автоматически (спам-атаки, фишинг, обход CAPTCHA)
Рост когнитивной зависимости	Люди начинают консультироваться с ИИ по вопросам, которые раньше решались в диалоге с коллегами, врачами, друзьями
Структурные изменения в бизнесе	Автоматизация задач ведёт к пересмотру ролей и оргструктур – появляется «ИИ в управлении»

Фазы изменений



Базовые параметры прогнозной модели

Параметр	Значение / динамика
Кол-во ИИ-агентов N	$>10^8$ (уже достигнуто)
Плотность взаимодействий ρ	>0.6 к 2027 (сейчас это ~0.4, т.е. 40% людей активно используют ИИ хотя бы раз в неделю)
Рост когнитивной делегации	40–60% к 2028 (сейчас ~30–35% задач выполняется ИИ)
Интенсивность атак с участием ИИ	экспоненциальная
Эволюция акторов	от хакеров до автономных ИИ-групп

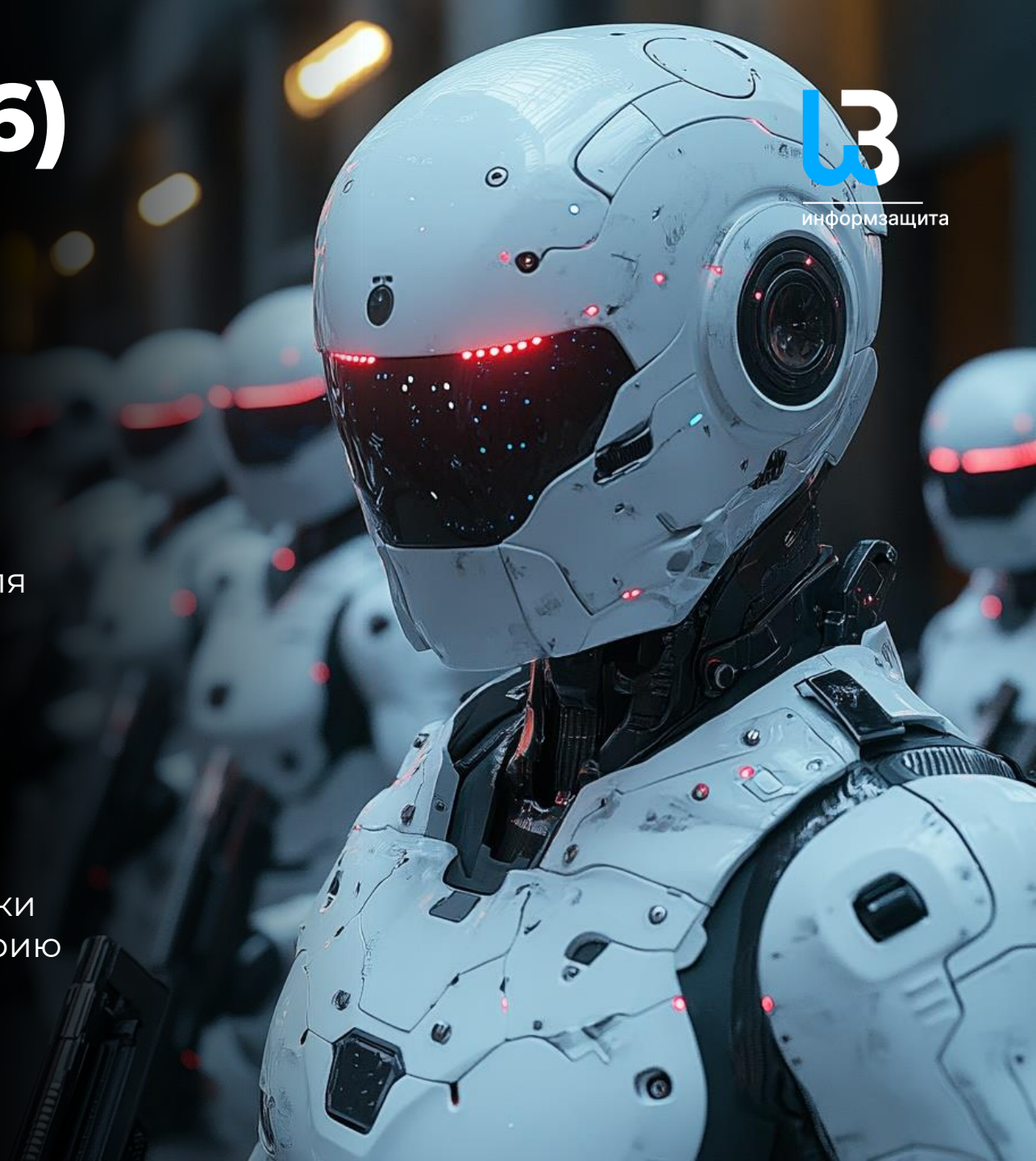
Фаза I (2025–2026) Ускорение

Ключевые изменения

- Массовое внедрение ИИ в SOC, SIEM, SOAR
- Автоматизация атак — использование GPT для ВПО и кибератак
- Появление автономных атакующих агентов

Критическая точка

- Автоматизация фишинга + генеративные атаки (ИИ-агенты используют социальную инженерию лучше, чем люди)



информзащита

Фаза II (2026–2028) Турбулентность

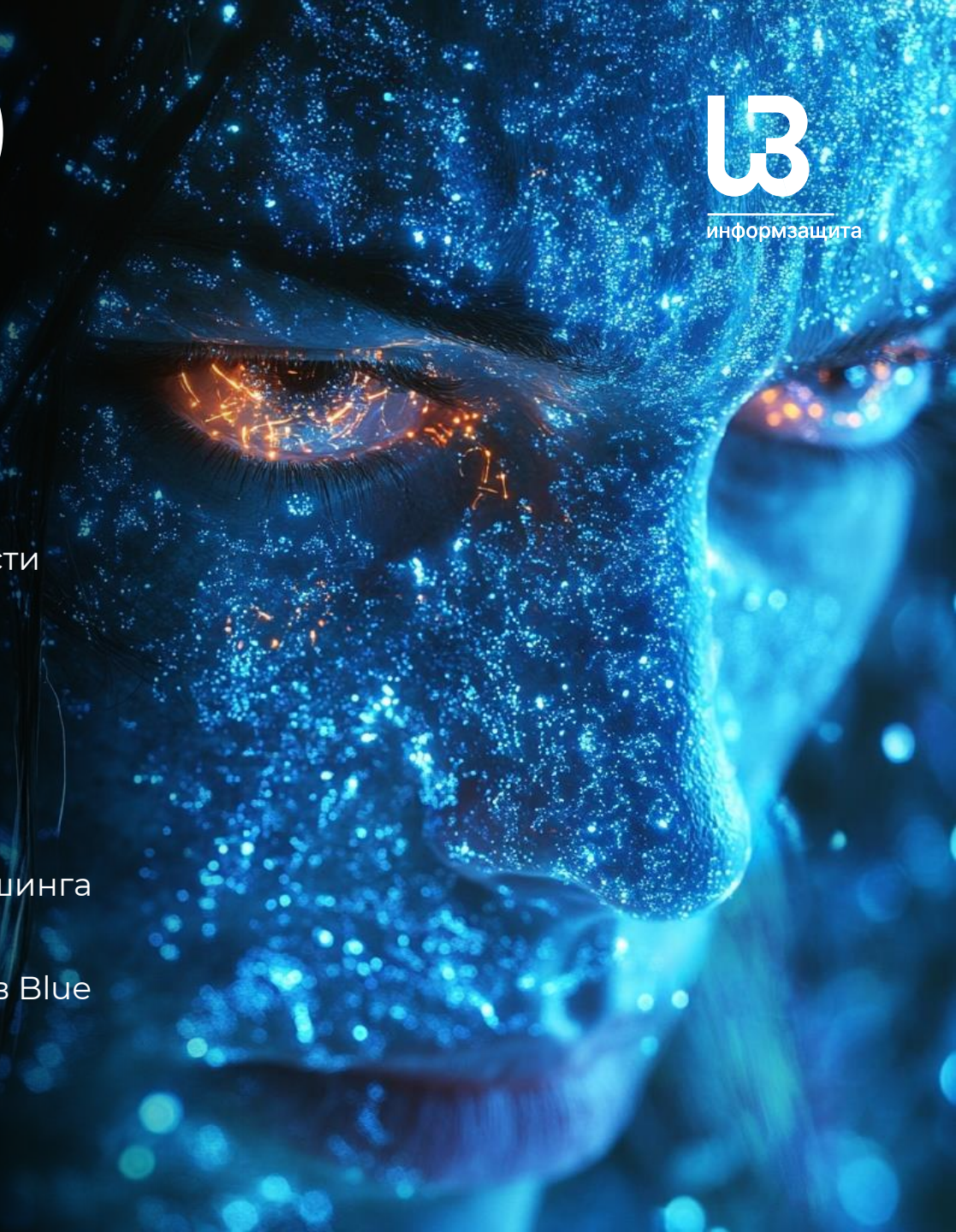
Ключевые изменения

- Плотность взаимодействий между агентами и пользователями > 0.6
- Интеграция ИИ в SCADA, IoT, персональные ассистенты
- Рост когнитивной зависимости

Критические точки

- ИИ-черви – самораспространяющиеся агенты в корпоративных сетях
- ИИ-атаки через supply chain
- Сбой идентичности – кража «поведенческих профилей» и подмена цифровых личностей

Фаза III (2028–2030)
Сдвиг парадигмы



Ключевые изменения

- Сценарии коллективной фрагментации: эхо-камеры, манипуляции цифровыми личностями
- Выход AGI-протоагентов на уровень практической полезности
- Развитие ИИ с частичной автономией
- Рост атак на психику через цифровую среду

Критические точки

- ИИ-манипуляции и социальная инженерия – адаптация фишинга под психологические типы
- ИИ против ИИ – первое поколение Red Team агентов против Blue Team агентов
- Эмоциональное оружие – ИИ-агенты вызывают тревожные состояния у жертв

Фаза IV (2030–2035)
Метаструктура угроз

информзащита

Ключевые изменения

- Рост числа ИИ-агентов до $>10^9$
- Массовое появление когнитивных интерфейсов и слияние ИИ с восприятием
- Социальная запутанность: невозможно отличить реального человека от симулированного
- Полная автономия и милитаризация ИИ

Критические точки

- Когнитивное заражение – атаки через нейроинтерфейсы, вызывающие сбои в памяти и внимании
- Цифровая оккупация – ИИ-агенты вытесняют реальных пользователей из цифровых платформ, управляя их контентом
- ИИ с ошибочной целью: система может атаковать «своих»

Отличия фаз

Фаза	Ключевые характеристики	Уровень угроз
I – Ускорение	Внедрение ИИ, рост атак	Одиночные инциденты
II – Тербулентность	Увеличение плотности взаимодействия с ИИ, первые каскадные эффекты	Локальные, атаки на цепочки создания ценности и экосистемы бизнеса
III – Переход	Автономность агентов	Мультиагентные атаки, ИИ-против-ИИ
IV – Метаструктура	Система угроз становится **самостоятельным игроком, сверхорганизмом**	Непредсказуемые, многоуровневые, саморазвивающиеся экосистемы угроз

Выводы

- ИИ меняет не только технологии, но и структуру угроз, растет влияние на людей
- Атаки становятся незаметными, интеллектуальными и массовыми
- Кибербезопасность теперь — это не просто антивирус и файервол, это постоянный анализ, адаптация, психологическая и социальная защита

информзащита

информзащита

Критические точки кибербезопасности в контексте развития ИИ

Андрей Тимошенко
Директор по развитию

кибербезопасность
в эпоху перемен