Цифровизация начинается с ИБ

Хачапуридзе Александр Георгиевич

Askona Life Group

МОСКВА

2025

Что Происходит?

01
Высокий уровень цифровизации

02
Атаки на разрушение инфраструктуры

03
Утечки данных

04
ИИ, LLM, ML и т.д.

05
Атаки на цепочку поставщиков

06
Дефицит кадров/ Человеческий фактор

Что Происходит?

Высокий уровень цифровизации

Industry 4.0

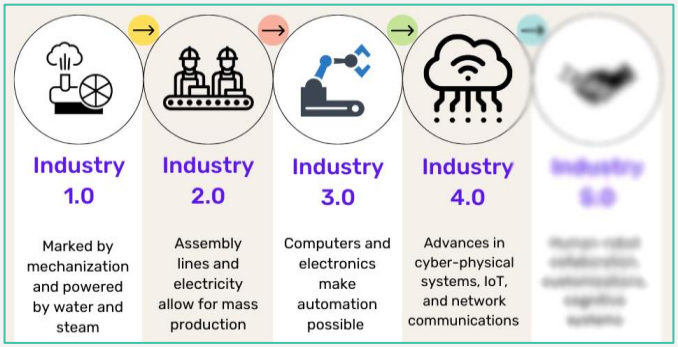
2011, Германия

Предполагает массовое внедрение ИТ в промышленность, масштабную автоматизацию бизнес-процессов и распространение искусственного интеллекта.

Industry 5.0

2017, Германия

предполагает синергию между людьми и автономными машинами



Что Происходит?

Атаки на разрушение инфраструктуры

+ 50% деструктивных атак
за 2024

2.5 раза больше кибератак, 130 000
за 2024

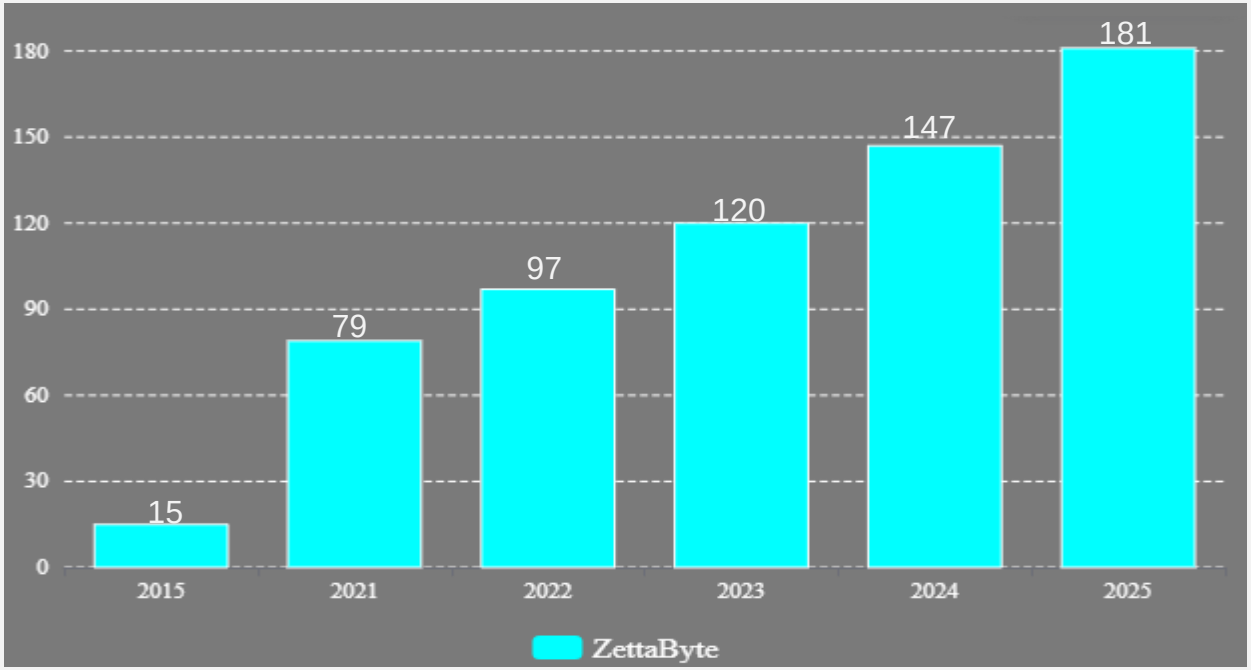
64% атак на КИИ
за 2024

60% атак это APT
за 2024

31% атак на ПРОМЫШЛЕННОСТЬ
за 2024

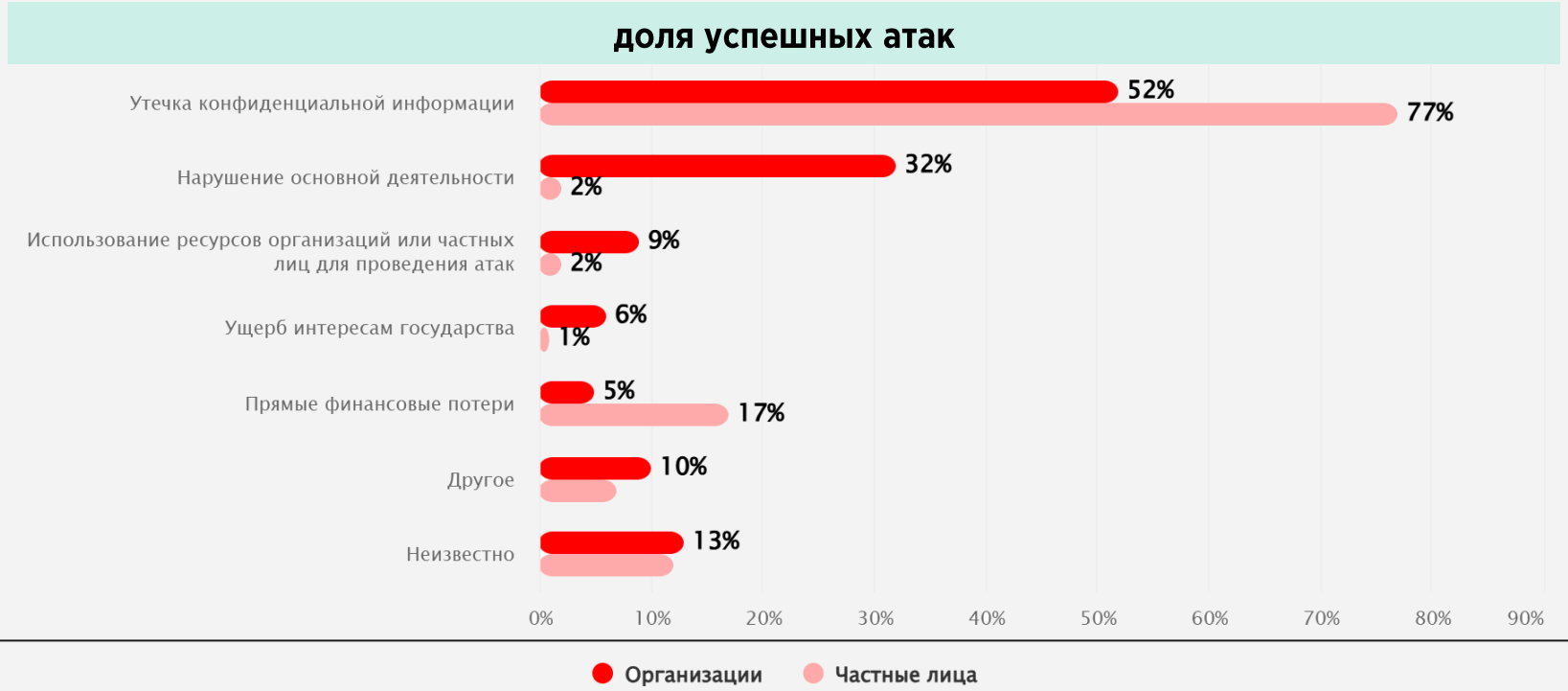
Что Происходит?

ИИ, LLM, ML и т.д.



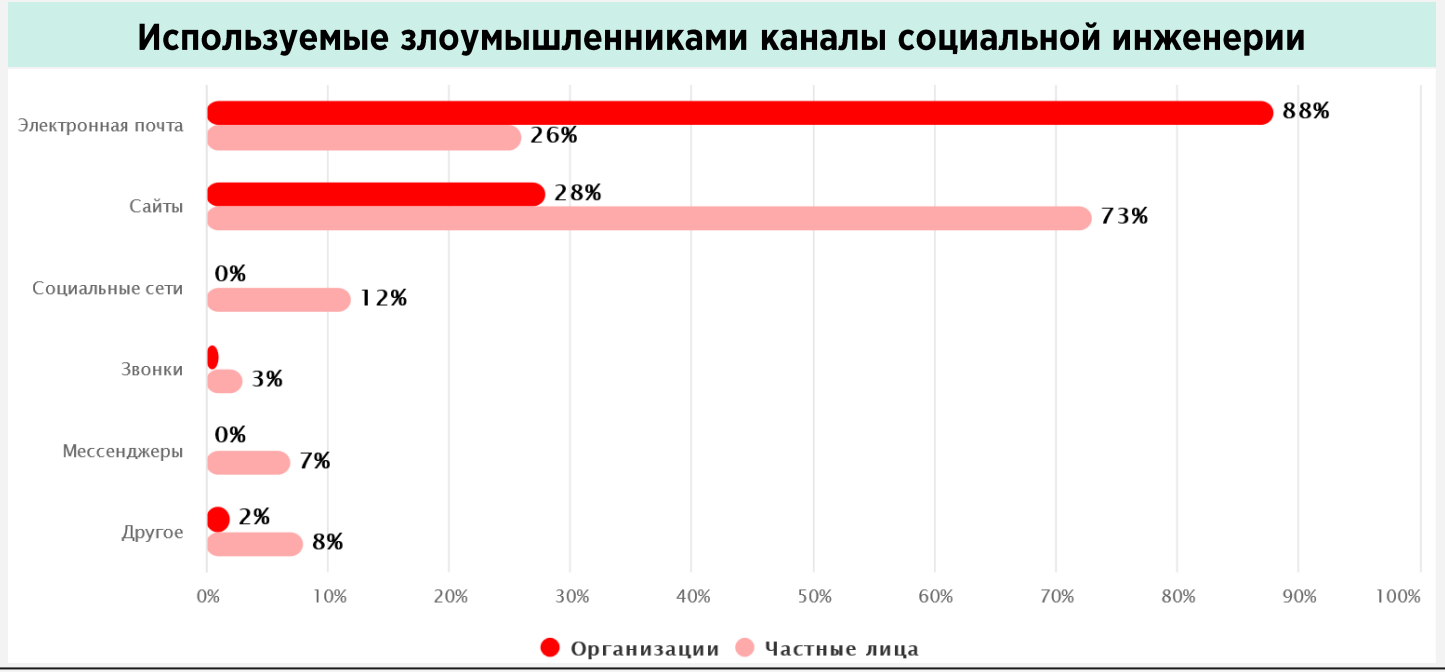
Что Происходит?

Утечки данных



Что Происходит?

Человеческий фактор



Причины

Традиционные проблемы ИБ

- ВЫСОКИЙ УРОВЕНЬ ЭВОЛЮЦИИ «УГРОЗ» И МАШТАБ «АТАК»
- Значительный рост применения концепции BYOD
- Размытие границы периметра
- Непрозрачность событий ИБ в корпоративной инфраструктуре предприятий
- Трудности с вопросом автоматизации всех процессов ИБ
- Интеграция ИБ-решений
- Гибкое масштабирование
- ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Что делать?

Кибер гигиена

Повышать уровень осведомлённости сотрудников

игровые кибермеханики для сотрудников

улучшить взаимодействие между HR- и ИБ-командами через обучение

оптимизировать ресурсы компании с помощью учебной системы

Что делать?

Автоматизация ИБ

Автоматизированные системы и сервисы

- экосистемы управления безопасностью
- ИИ и LLM, системы в продуктах ИБ
- сервисы ИБ – коммерческий SOC, SaaS, IaaS, PaaS
- оптимизация технологий и процессов ИБ

pt

R-Vision

k

SOLAR

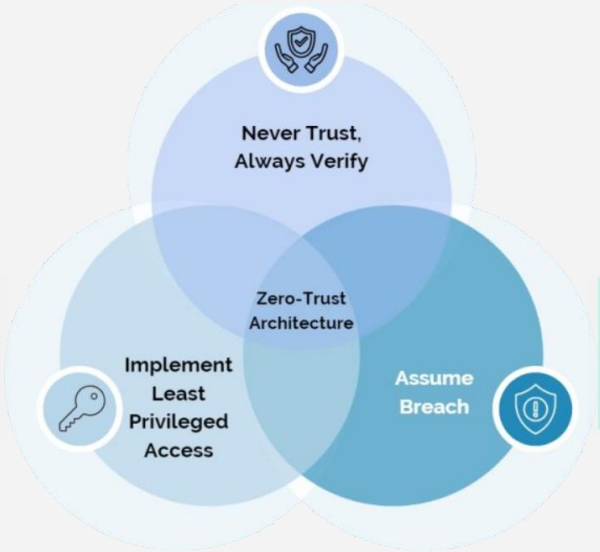
MTS AI

Что делать?

ZTA

Zero Trust Architecture

никогда не доверяй, всегда проверяй



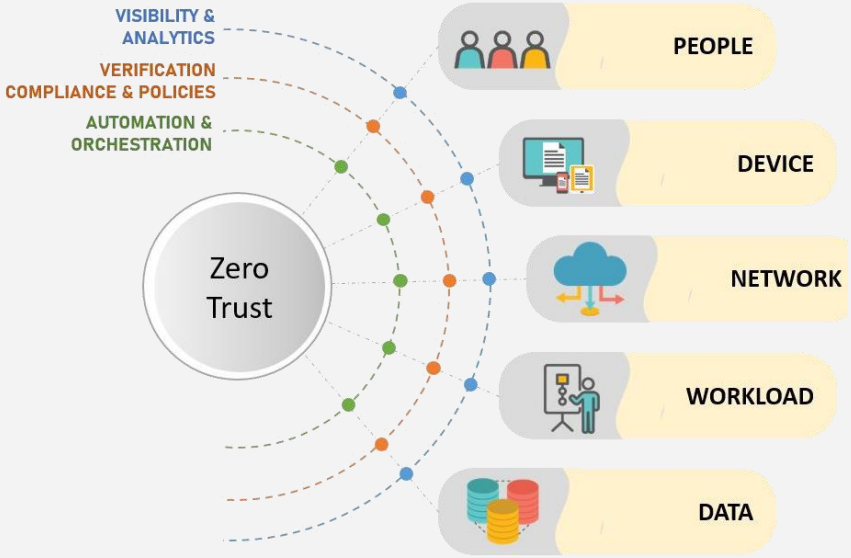
привилегии с наименьшими правами

нарушение уже произошло

Что делать?

Zero Trust Architecture

архитектурная модель безопасной информационной системы. Которая по умолчанию лишена доверенных объектов или субъектов, доверенных зон, доверенных связей или процессов. Модель предполагает наличие минимальных привилегий, обязательной сегментации, а также непрерывную проверку и аутентификацию.



Что делать?

Zero Trust Architecture

1994

Стивен Пол Марш – вводит понятие «нулевое доверие»

Sun Microsystems – инженеры описывают защиту сети как «скорлупу яйца»

2009

Operation Aurora – APT атака на Google. Организована Китайской группировкой

2010

Google начинает внедрять архитектуру ZTA, известную как BeyondCorp

Джон Киндерваг разработал оригинальную модель ZT

2020

NIST SP 800-207 – NIST опубликовал стандарт, описывающий ZTA

Что делать?

Принципы Zero Trust

от Google и Джона Киндервага

Google

Сегментация – изоляция приложений, сервисов, потоков, данных, узлов и пользователей

Контроль доступа – доступ к ресурсам только по необходимости

Видимость – непрерывный контроль за доступами и журналирование

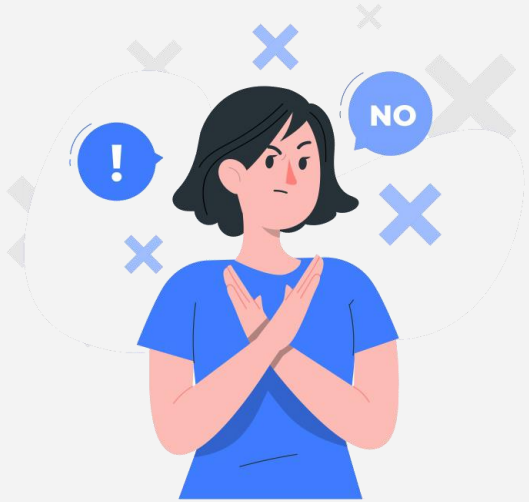
Что делать?

ZTA это не:

НЕ ПРОДУКТ
ZTA не продаётся как готовое решение

НЕ ПРОТОКОЛ
для ZTA нет регламентирующих правил и требований

НЕ ТЕХНОЛОГИЯ
нет технологических процессов или правил обеспечивающих достижения ZTA



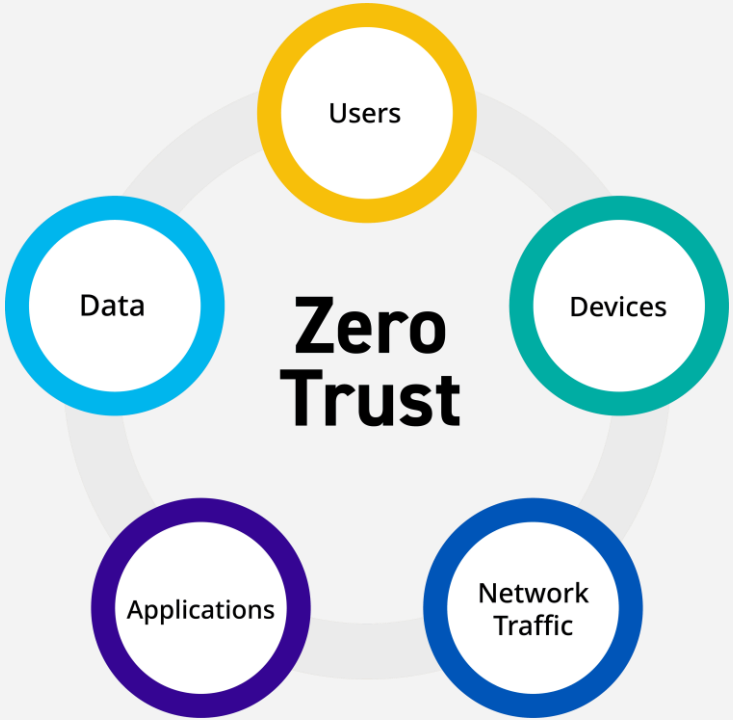
Что делать?

ZTA это:

АРХИТЕКТУРНАЯ МОДЕЛЬ
подход к проектированию ИС в парадигме нулевого доверия

НАБОР ПОЛИТИК И ПРАВИЛ
соблюдение правил обеспечивающих нулевое доверие

ЗАЩИЩЕННАЯ ЦИФОРОВАЯ СИСТЕМА
Система в которой нет доверенных узлов, пользователей, данных, потоков.

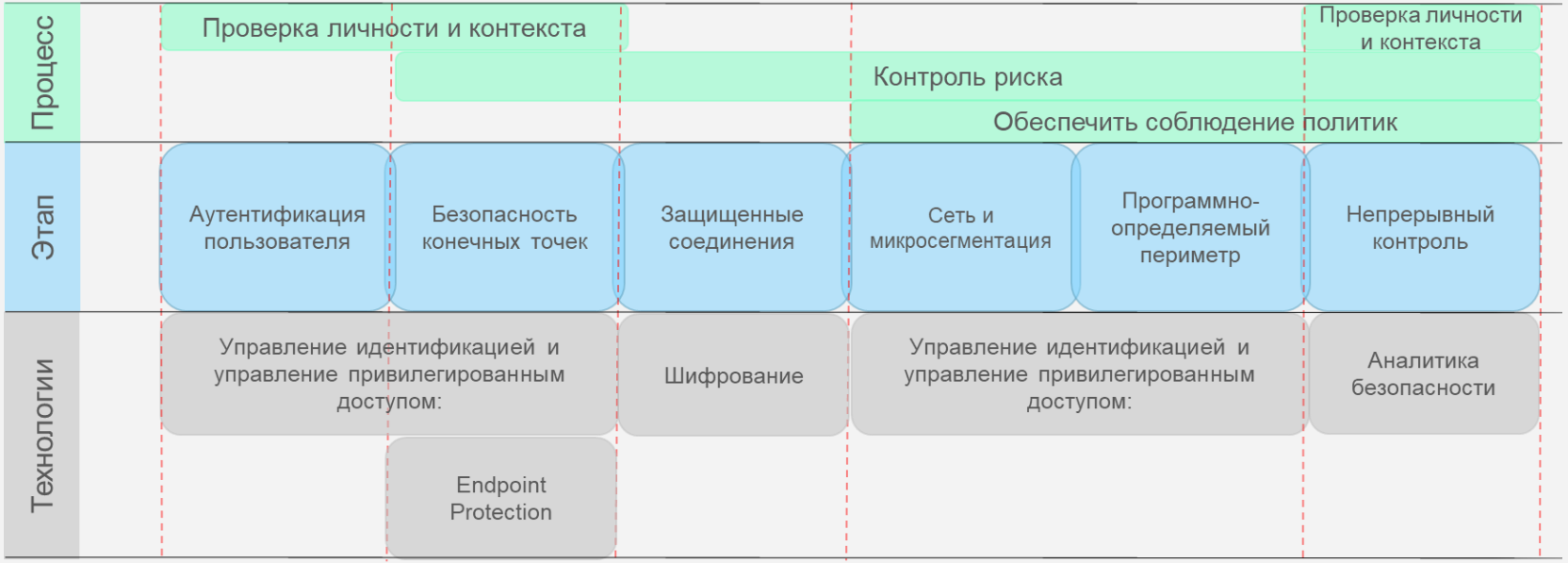


Как сделать?

ZTA структура

Как сделать?

ZTA структура



Как сделать?

ZTA риски

- Подделка аутентификации и ложный доступ
- Отказ в обслуживании
- «Не видимость сети»
- Устранение возникших «дыр»
- Хранение информации ZTA
- Зависимость бизнеса от конкретных решений
- Уязвимость автоматизации управления ZTA

Как сделать?

ZTA сложности

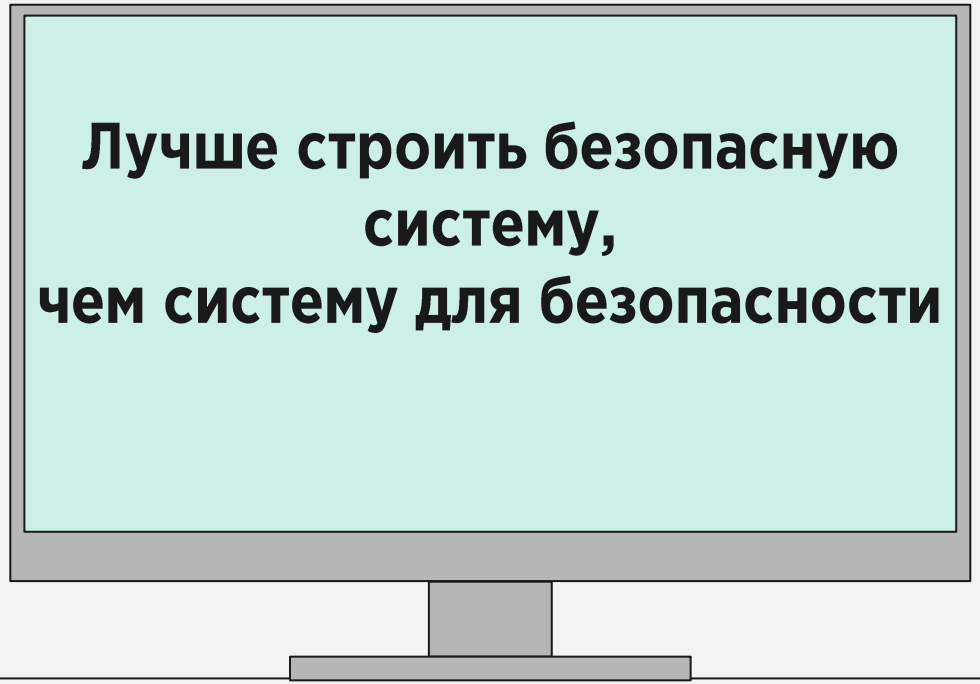
- Масштабирование в сложных средах
- Используемые инструменты
- Отказ от устаревших систем
- Устранение возникших «дыр»
- Баланс безопасности
- Смена мышления
- Финансирование и затраты

Как сделать?

ZTA преимущества

- «Врождённая» защищенность целевой системы
- Снижение внутренних угроз
- Эффективное реагирование на инцидент безопасности
- Минимизация поверхности атаки и зоны поражения
- Улучшенный мониторинг и детальный контроль
- Масштабируемость и максимальная совместимость
- Ориентированная на перспективу
- Улучшает качество бизнес процессов

Заключение


Лучше строить безопасную
систему,
чем систему для безопасности

Спасибо за внимание

Хачапуридзе Александр Георгиевич

Askona Life Group

МОСКВА

2025