Yandex Cloud

Код ИБ: итоги 2025

Защита данных 2025:
от угроз — к архитектуре доверия

Александр Мизерин,
Information security and Compliance Expert

Данные — главная цель

76%

атак целятся в облачные хранилища (S3) и базы данных

Источник: «Анализ киберугроз в облачных и гибридных инфраструктурах за первое полугодие 2025» https://yandex.cloud/ru/blog/reflected-attacks-h1-2025

Три ключевые уязвимости

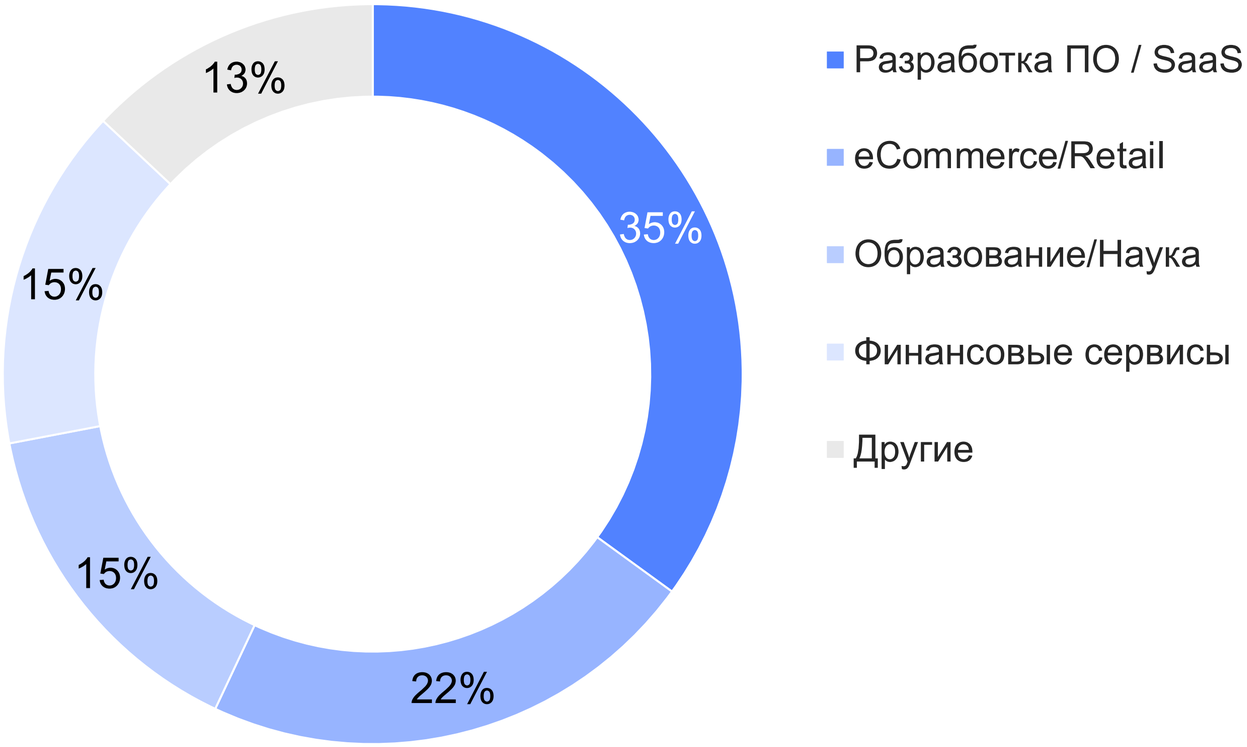
- Слабые пароли
- Статичные секреты
- Ошибки конфигурации, открывающие прямой доступ к базам данным или S3

+ Инсайдерские угрозы

Но Облако обеспечивает полное логирование действий

Главные цели кибератак в 2025

Распределение атак по отраслям



Ключевые наблюдения

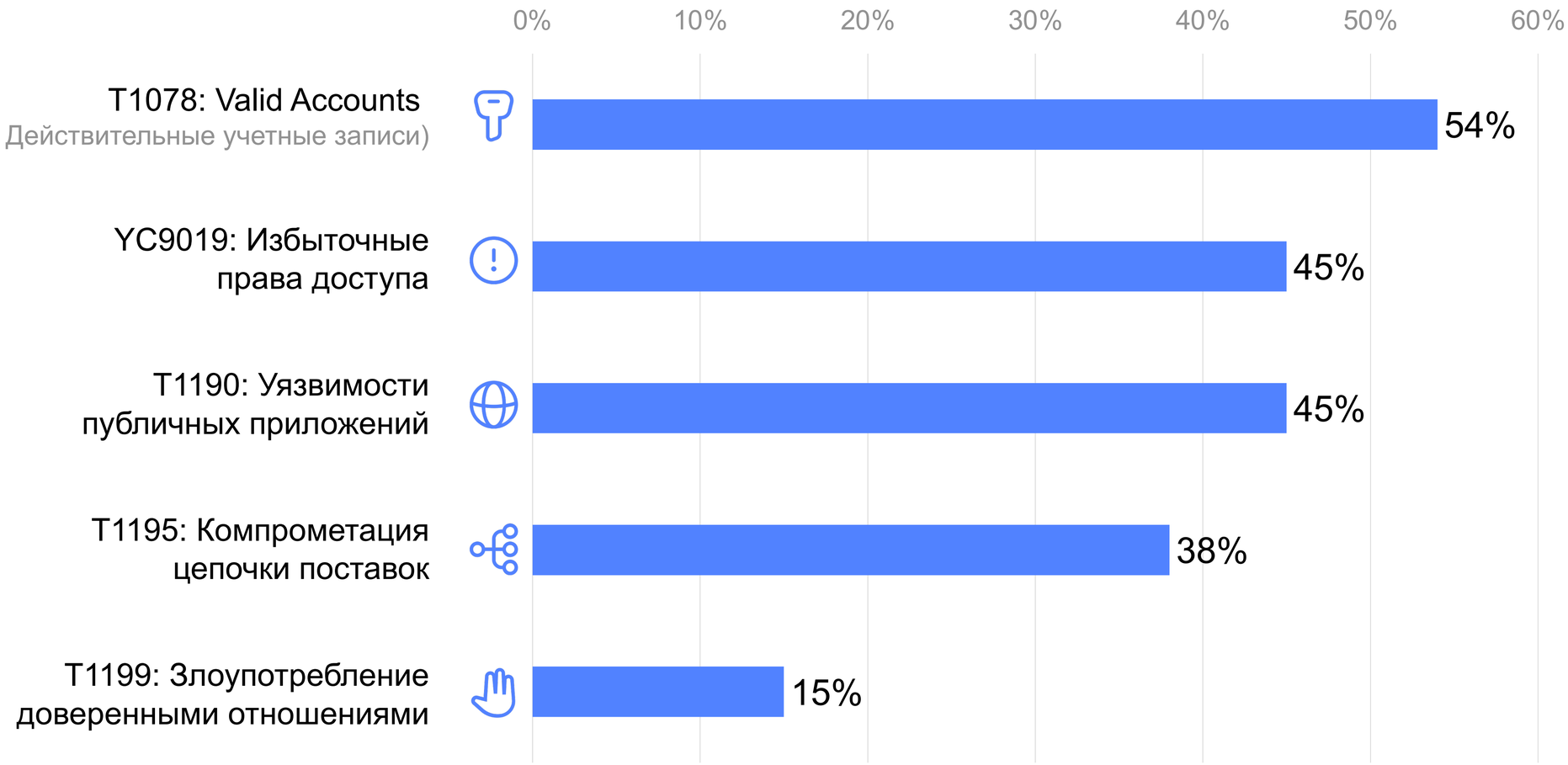
- SaaS-разработчики (35%)
  - Главная цель для атак через цепочку поставок
  - Поиск секретов для последующих атак на клиентов
- Ритейл (22%)

  Фокус на персональных данных и платежной информации
- Финансы & Образование
  - Атаки с шифрованием данных и требованием выкупа
  - Кража интеллектуальной собственности

Источник: «Анализ киберугроз в облачных и гибридных инфраструктурах за первое полугодие 2025» https://yandex.cloud/ru/blog/reflected-attacks-h1-2025

ТОП-5 техник атак по MITRE ATT&CK®

По частоте использования (1H2025)



Источник: «Анализ киберугроз в облачных и гибридных инфраструктурах за первое полугодие 2025» https://yandex.cloud/ru/blog/reflected-attacks-h1-2025

Статистика по безопасности самой платформы за 2024 год

1,3 млрд ₽

Общее количество инвестиций

Было 820 млн ₽

14

Внешних аудитов ИБ

Было 12

1,5 млн ₽

Выплаты Bug Bounty

Было 6 млн ₽

17

сервисов безопасности

Было 10

~130

Человек в Security

Было 100

>1500

часов Red Team

Было 1500

Yandex Cloud учитывает требования международных и национальных стандартов

Cloud Security Alliance

Security, Trust, Assurance and Risk (STAR) по уровню Level 1

ГОСТ Р 57580.1-2017

Безопасность финансовых операций

Реестр программного обеспечения

Запись в реестре
№ 9286 от 20.02.2021

152-ФЗ, УЗ-1

Аттестат соответствия по требованиям 21-го приказа ФСТЭК

Стандарты ISO

ISO 27001, ISO 27017, ISO 27018 и ISO 27701,
ISO 42001 NEW!

Стандарты PCI

PCI DSS v4
Для ЦОД и облачных сервисов, PCI PIN и PCI 3DS

GDPR

Общий регламент о защите данных в Европейской зоне

Доступные инструменты обеспечения безопасности

Руководства и гайды

- Стандарт по защите облачной инфраструктуры Yandex Cloud
- Документация и чек-листы
- Бюллетени безопасности

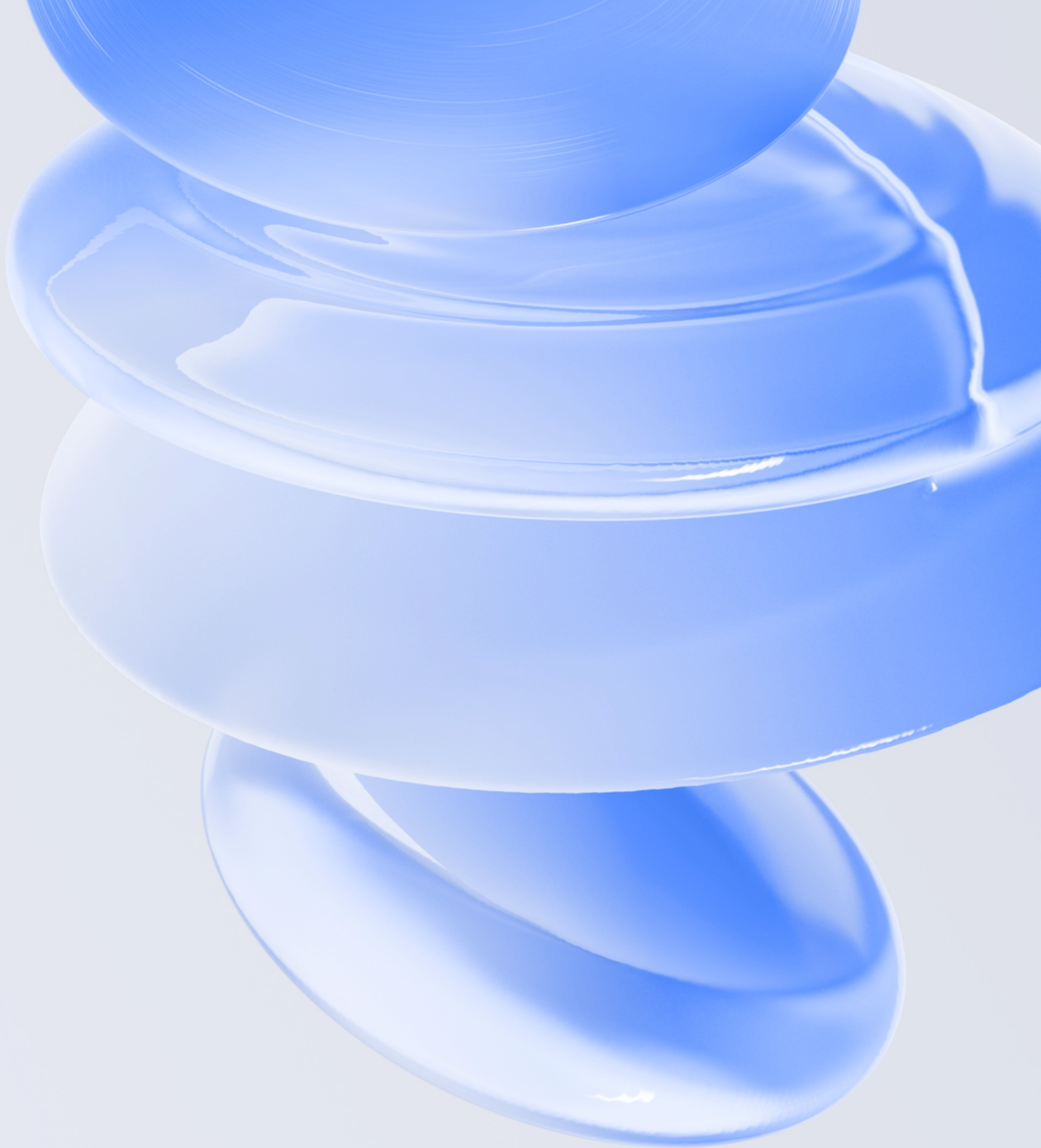
Security Solution Library

- Готовые сценарии и примеры
- Решения на базе сервисов облака
- Решения с использованием сторонних средств защиты

Углублённое обучение

Курсы по безопасности облачных платформ

Cloud Trust



Доверяй облакам,
но проверяй безопасность

Центр экспертизы Cloud Trust

- Готовые решения по облачной безопасности
- Соответствие требованиям безопасности
- Консалтинг по безопасной миграции цифровых продуктов

ИИ и безопасность: обоюдное влияние

Двустороннее движение

- Новые угрозы:
  ИИ создает уникальные векторы атак
- Новые защиты:
  ИИ усиливает безопасность

Результат внедрения ИИ-ассистента в SOC: MTTR ↓ 30%

- Автосуммаризация инцидентов
- Генерация контекстных плейбуков
- Анализ данных SIEM в реальном времени

Главные облачные риски (H1 2025)

- Компрометация учетных записей
- Злоупотребление доступом
- Ошибки конфигурации

Источник: «Анализ киберугроз в облачных и гибридных инфраструктурах за первое полугодие 2025» https://yandex.cloud/ru/blog/reflected-attacks-h1-2025

Отвечу на ваши вопросы

Александр Мизерин,
Information security and Compliance Expert
mizerinas@yandex-team.ru

t.me/mizerinas