

ИНФОСИСТЕМЫ ДЖЕТ



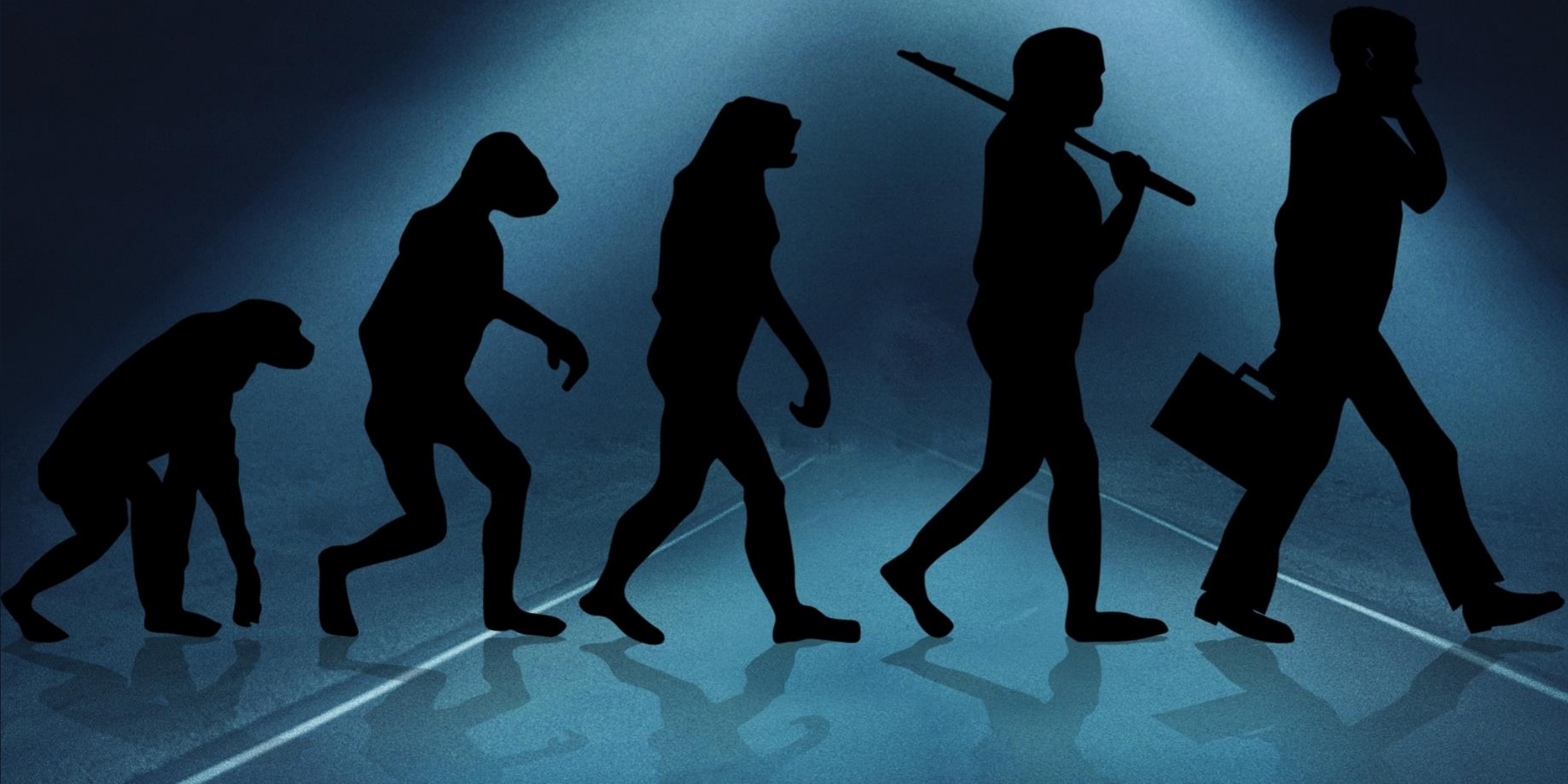
Л Е Т

ФОРМИРУЕМ ТРЕНДЫ  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ

# Сегодня и завтра информационной безопасности. Тенденции рынка ИБ

Андрей Янкин,  
руководитель отдела консалтинга  
Центра информационной безопасности

# Тенденции





# ИБ становится ближе к бизнесу

- ✓ Риски ИБ начинают восприниматься менеджментом, как неотъемлемые риски бизнеса
- ✓ ИБ теперь не только Compliance
- ✓ Интеграция с ЭБ и ФБ
- ✓ Грань между антифродом и ИБ стирается
- ✓ Служба ИБ не всегда готова



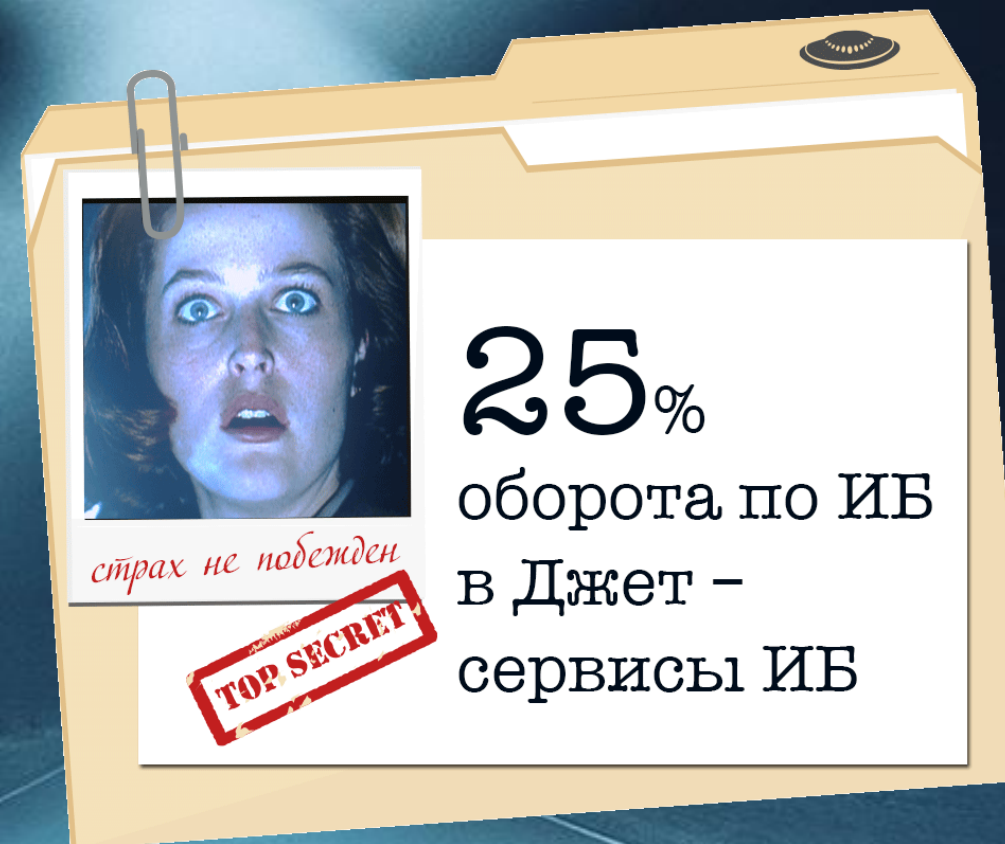
# Таргетированные атаки

- ✓ Таргетированные атаки стали прозаичным явлением: от шпионских историй к массовому воровству денег
- ✓ Число атак на финансовые учреждения выросло на порядок
- ✓ Социальная инженерия – абсолютно массовое явление





- ✓ Страх еще не побежден
- ✓ Период юности аутсорсинга ИБ:
  - Не сформированы услуги
  - Малая конкуренция
  - Нет понимания SLA
- ✓ На рынке дефицит квалифицированных кадров
- ✓ Серьезный подход к ИБ требует узких специализаций



- ✓ Против угроз единым фронтом:
  - FinCERT, ГосСОПКА
  - Коммерческие CERT
- ✓ Развитие двусторонних связей: не только получать данные, но и делиться находками
- ✓ Строительство SOC: впереди финансовый сектор, крупная промышленность, ТЭК



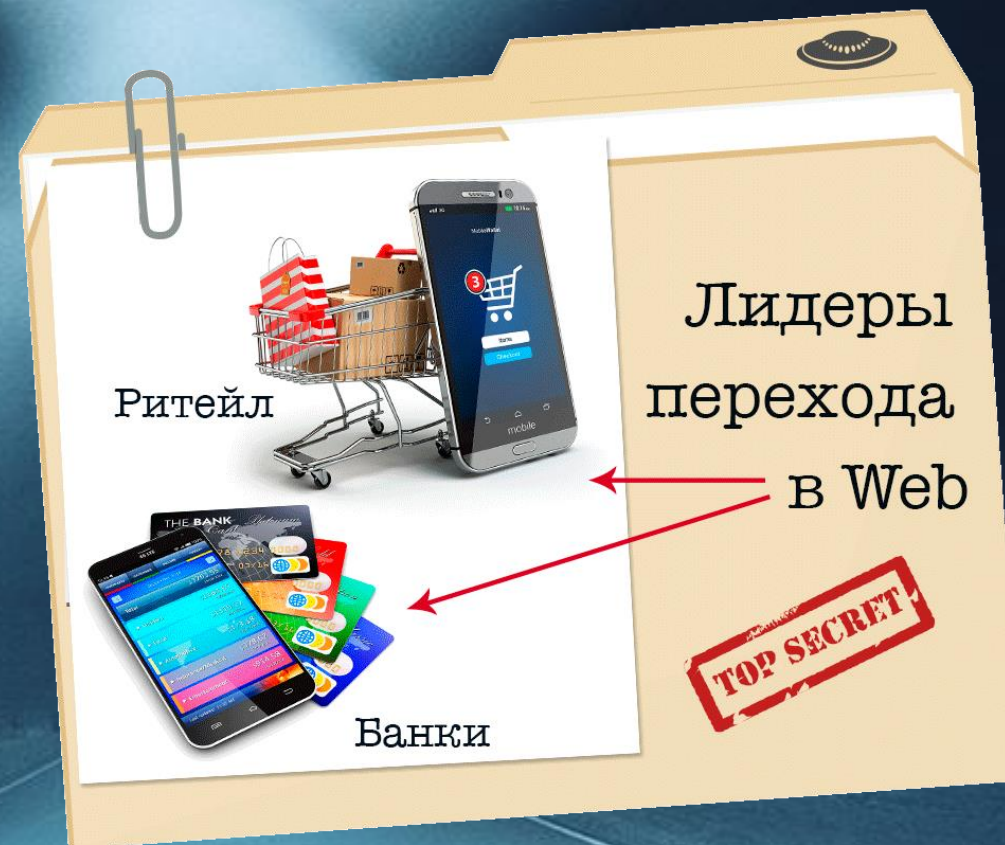


- ✓ Рост понимания реальности рисков
- ✓ Усиление давления регуляторов
- ✓ Существенное развитие рынка средств защиты АСУ ТП
- ✓ Термин «ИБ АСУ ТП» должен исчезнуть из употребления
- ✓ Рынок специализированной ИБ могут занять не ИТ-интеграторы, а игроки рынка SCADA



# Рост интереса к безопасности Web

- ✓ Массовый переход в Web
- ✓ Мобильные клиенты, бизнес-приложения – тоже Web
- ✓ Атаки: выведение из строя, взлом, мошенничество
- ✓ Атаки на крупные площадки идут постоянно
- ✓ Стремительный рост рынков WAF, защиты от DDoS, пентестов, анализа кода





Самописное ПО,  
заказная разработка  
– мишень для  
хакеров №1



Исследование наших  
экспертов:

Обследовано

**58** банковских мобильных  
приложений

**98%** имеют уязвимости

**40%** имеют критические  
уязвимости



Производители:

Bug-Bounty программы,  
анализ кода



Заказчики:

Необходимость  
внешнего контроля

Отсутствие  
компетенций

Выход: сервис  
анализа кода,  
пентесты



# Прогнозы





- ✓ До ИБ интернета вещей еще далеко. Сначала возникнут массовые угрозы
- ✓ Шутки, PoC на конференциях, выведение устройств из строя, атаки на людей – юность темы



- ✓ Залог роста проблемы: массовость технологий и понятные схемы монетизации
  - Массовость оборудования с подключением к Интернет: бытовая техника, автомобили, умный дом и т.д.
  - Унификация прошивок
  - Снижение вреда владельцу
  - Использование устройств для рассылки спама, DDoS-атак





- ✓ Несмотря на кажущуюся заезженность, тема защиты ПДн в России совершенно не развита:
  - Только Compliance
  - Реальной защитой ПДн почти никто не занят
- ✓ Аналог: банковская отрасль перешла от Compliance к реальной безопасности





- ✓ Залог смены подхода: реальные риски
  - Крупные штрафы за утечки, а не за несоответствие требованиям
  - Судебная защита прав пострадавших
  - Серьезный финансовый и репутационный ущерб
- ✓ Акцент на защите действительно критичных данных
- ✓ Приход понимания того, что остальные данные априори общедоступны





- ✓ Вредоносные сервисы станут понятнее для бизнеса:
  - Удобство для пользователя
  - Надежность
  - Борьба за репутацию
  - Анонимность
  - Мощный маркетинг
- ✓ Рост объема атак как компонента корпоративной борьбы



## ✓ Черная BigData: покупка информации в нелегальных банках данных

- Индивидуальный взлом — слишком дорого, долго и сложно
- Отдельные базы гос. органов давно продаются с регулярным обновлением
- Переход к сервису «одного окна»: агрегаторы данных
- Назначение: конкурентная борьба, маркетинг, политика и т.д.





ИНФОСИСТЕМЫ ДЖЕТ



Л Е Т

ФОРМИРУЕМ ТРЕНДЫ  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ

Спасибо за внимание!