



Банк России

Центральный банк Российской Федерации



# Перспективы развития финансовых рынков с точки зрения регулятора

VIII Уральский форум «Информационная безопасность финансовой сферы»

С.А. Швецов, Первый заместитель  
Председателя Банка России

17.02.2016

# Демографический фактор как драйвер дигитализации

Y

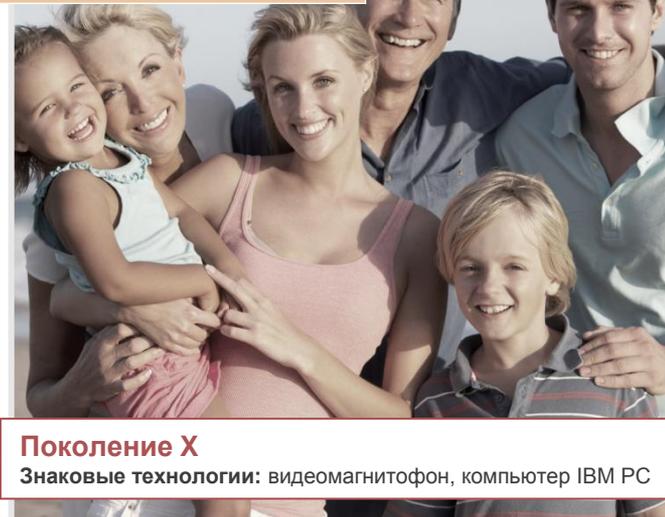
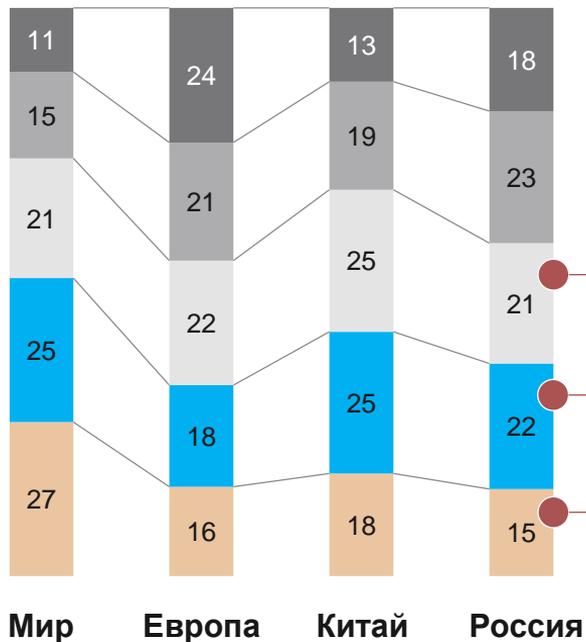
1/3 специалистов на финансовом рынке – представители поколения Y

Z

Представители поколения Z начинают выходить на рынок труда

Поколение Год рождения Доля поколений в населении, %

Старшие поколения	До 1946
«Бэби-бумеры»	1946-64
Поколение X	1964-80
Поколение Y	1980-2000
Поколение Z	1995+



## Поколение X

**Знаковые технологии:** видеомэгафон, компьютер IBM PC

## Поколение Y

**Знаковые технологии:** Интернет, e-mail, мобильный телефон, Google, iPhone

## Поколение Z

**Знаковые технологии:** Facebook, Twitter, Tinder, Foursquare, Instagram, Google Glass, облачные сервисы

## Цели и контрольные показатели

### Основные цели дорожной карты

- ✓ последовательное уменьшение доли и создание предпосылок для **устранения бумажного документооборота** на финансовом рынке
- ✓ улучшение механизмов взаимодействия Банка России с участниками финансового рынка и **создание непрерывных цепочек электронного взаимодействия всех вовлеченных участников**
- ✓ повышение доступности финансовых услуг и инструментов: **равные возможности по доступу** на финансовый рынок, к финансовым услугам и инструментам для граждан и участников рынка
- ✓ повышение **удобства работы, уровня доверия и психологического комфорта** граждан при использовании электронных способов взаимодействия с финансовыми организациями
- ✓ повышение **прозрачности и безопасности операций** в сфере предоставления розничных финансовых услуг
- ✓ повышение эффективности мер по **противодействию легализации (отмыванию) доходов**, полученных преступным путем, и финансированию терроризма путем реализации риск-ориентированного подхода к вопросам идентификации
- ✓ повышение операционной эффективности, **снижение непрофильных затрат** финансовых организаций

### Целевые контрольные показатели

Наименование показателя	Текущее значение	2016	2018
уровень затрат на бумажный документооборот, в долях  <b>-30%</b>	100	85	70
доля продуктов и услуг, доступных клиентам финансовых организаций в электронном виде, в общем ассортименте финансовых продуктов и услуг  <b>+67%</b>	18	36	85
востребованность услуг и сервисов, представляемых в электронном виде, в долях  <b>+43%</b>	22	40	65
доверие к безопасности пользователей электронных технологий и сервисов, в долях  <b>+35%</b>	25	40	60



**29 трлн руб.**

объем безналичных платежей, совершенных физическими лицами в 2014 году

**239,6 млн**

число карт на руках у физических лиц за 9 месяцев 2015 года

**66%**

доля субъектов малого и среднего бизнеса, использующих интернет- и мобильный банкинг

**3,1 раз**

рост числа активных клиентов DMA/SMA за 2014-2015

**Robo-advisor****Big Data проекты**

# Традиционное понимание киберугроз и борьбы с ними

- **4 млн** – число финансовых счетов, затронутых в результате IT сбоя в 2014 году
- **\$ 3 трлн к 2020 году** – прогнозируемые убытки от промедления во внедрении адекватных мер кибербезопасности



## Драйверы для киберугроз

- Стоимость как определяющий фактор при инвестировании в кибербезопасность
- Недостаток понимания рисков вовлеченности в киберсреду
- Несовершенство правовой среды для применения санкций в отношении нарушителей
- Быстрое развитие технологий VS догоняющий характер развития средств защиты



## 6 компонентов кибербезопасности:

- Внедрение практики кибергигиены
- Выстраивание механизмов обнаружения и реагирования
- Обмен информацией с коллегами по отрасли
- Ориентация на лучшие практики и рекомендации регулятора
- Установка систем получения разведывательной информации о внешних угрозах
- Требование соблюдения норм кибербезопасности от контрагентов



Получение финансовой выгоды перестало быть единственной прямой целью



Новые тренды: подрыв деловой активности, удар по доброму имени и репутации (Name and Shame)



**69%**  
взломов выявлены не внутри самой организации



**100%**  
взломанных устройств имели самую передовую антивирусную защиту



**\$ 3,5 млн**  
средняя сумма ущерба от взлома

Почему недостаточно управлять  
рисками и соответствовать  
требованиям (Governance, Risk and  
Compliance, GRC)?

Успех GRC базируется на возможности  
опередить противника



Когда Вы – цель,  
от противника не убежать

Почему недостаточно управлять  
рисками и соответствовать  
требованиям (Governance, Risk and  
Compliance, GRC)?

GRC предполагает, что  
широкомасштабные угрозы и выглядят  
грандиозно

Масштабные взломы являются наиболее  
сложными в плане их обнаружения



# 3

Почему недостаточно управлять  
рисками и соответствовать  
требованиям (Governance, Risk and  
Compliance, GRC)?

GRC предполагает, что управление  
рисками – лучшее средство надежной  
защиты

Атакующие вписываются в рамки  
«допустимого риска», чтобы добраться до  
Вас

Источник: фотоархив ТАСС



# Этапы достижения киберустойчивости

