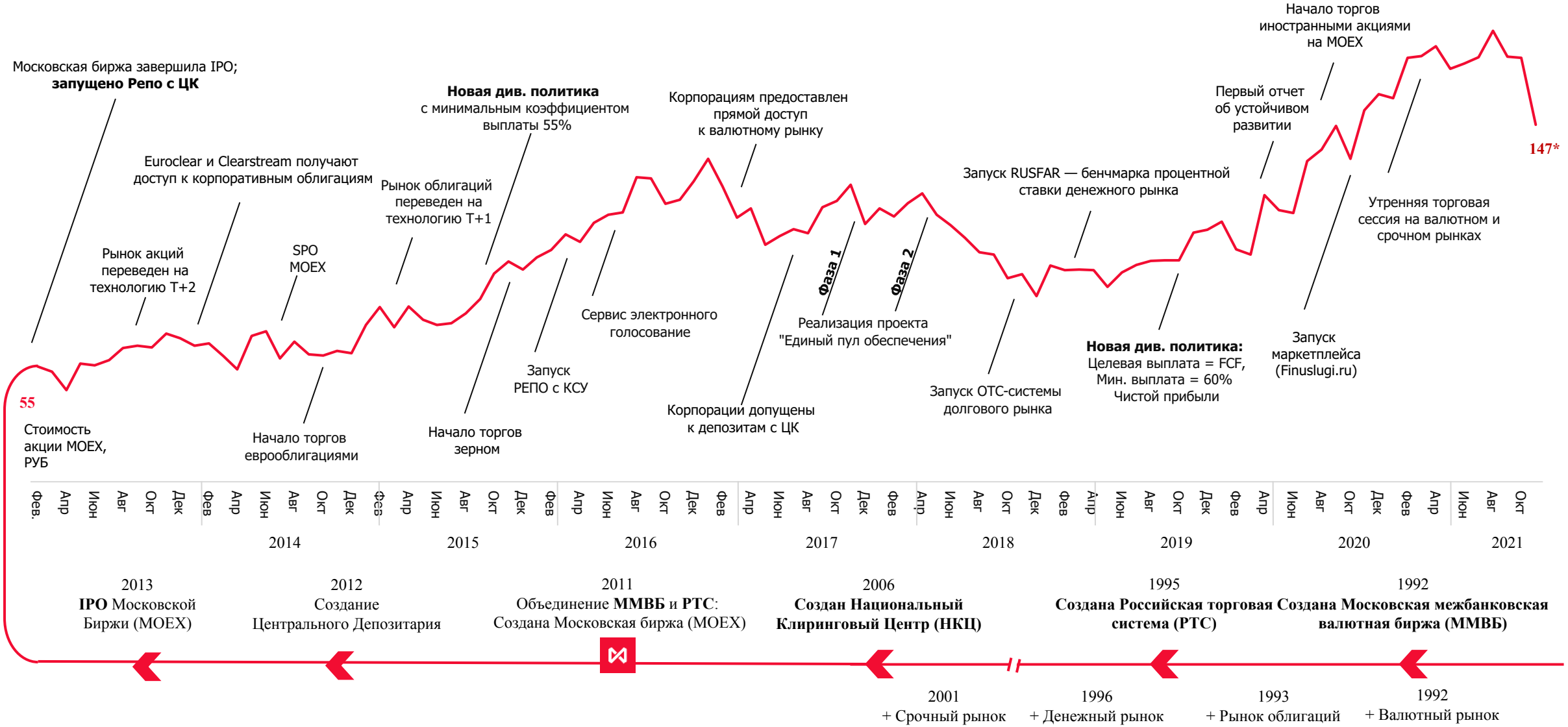
Безопасная разработка

ПОДГОТОВЛЕНО: СЕРГЕЙ ДЕМИДОВ

Кто мы?

История Московской Биржи



*Цена акции на 12.01.2022

Структура

MOEX GROUP

ФИН УСЛУГИ

Торги

Клиринг

Расчеты

НТБ
Товарная биржа

Московская Биржа
Фондовый рынок
Валютный рынок
Денежный рынок
Срочный рынок

НКО НКЦ (АО)
Клиринговый центр
Центральный контрагент на всех рынках

НКО АО НРД
Центральный депозитарий
Расчетный центр

Физические лица

Профессиональные участники рынка ценных бумаг

Клиенты участников торгов

Банки

Компании реального сектора

Разработчики ПО

ФОИВ’ы

ИТ инфраструктура, телекоммуникации, разработка ПО

Структура Группы «Московская Биржа»

Инфраструктура

Инфраструктура Московской Биржи – инструмент **денежно-кредитной политики Банка России**, а также инвестирования средств бюджета и пенсионных фондов и регулирования рынка зерна

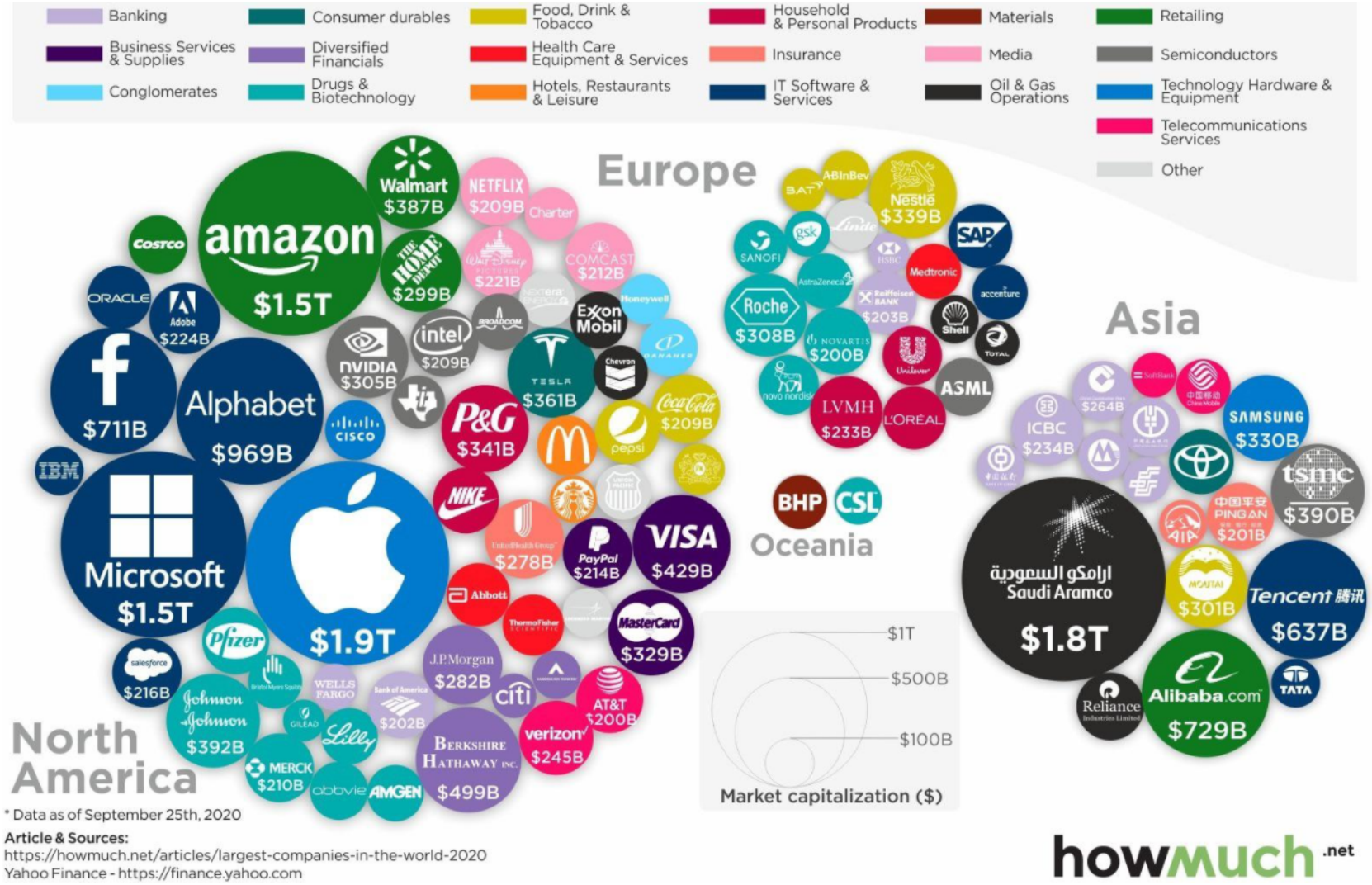
Центральный Банк России	▪ Денежно-кредитная политика	▪ Валютные операции (спот/своп) *(с 1992)* ▪ Прямое РЕПО с Банком России *(с 1996)* ▪ Депозитные и кредитные операции *(с 2004)* ▪ Облигации Банка России *(с 2004)*	2,6 трлн руб., -41% к 2019 2,8 трлн руб., +10 раз к 2019 40,2 трлн руб., -11% к 2019 5,2 трлн руб., -15% к 2019
Министерство Финансов	▪ Размещение государственных облигаций	▪ Рынок государственных облигаций *(с 1993)*	5,3 трлн руб., 158% к 2019
Федеральное Казначейство	▪ Инвестирование средств бюджета	▪ Депозитные операции *(с 2012)* ▪ РЕПО с Федеральным Казначейством *(с 2019)* ▪ Депозитные аукционы с ЦК по размещению средств единого казначейского счета *(с января 2021)*	6,7 трлн руб., -7% к 2019 22,3 трлн руб., +1000 раз к 2019
Пенсионный Фонд России (ПФР)	▪ Инвестирование пенсионных средств под управлением ПФР	▪ Депозитные операции *(с 2013)*	202 млрд руб., -30% к 2019
Внешэкономбанк (ВЭБ)	▪ Инвестирование пенсионных средств под управлением ВЭБ	▪ Депозитные аукционы *(с 2009)*	280 млрд руб., -20% к 2019
Министерство сельского хозяйства	▪ Регулирование рынка зерна	▪ Интервенции на рынке зерна *(с 2002)* ▪ Расчет трех ценовых индексов зерновых культур: пшеницы, ячменя и кукурузы *(с апреля 2021)*	21 млрд руб., +107% к 2019

Безопасная разработка

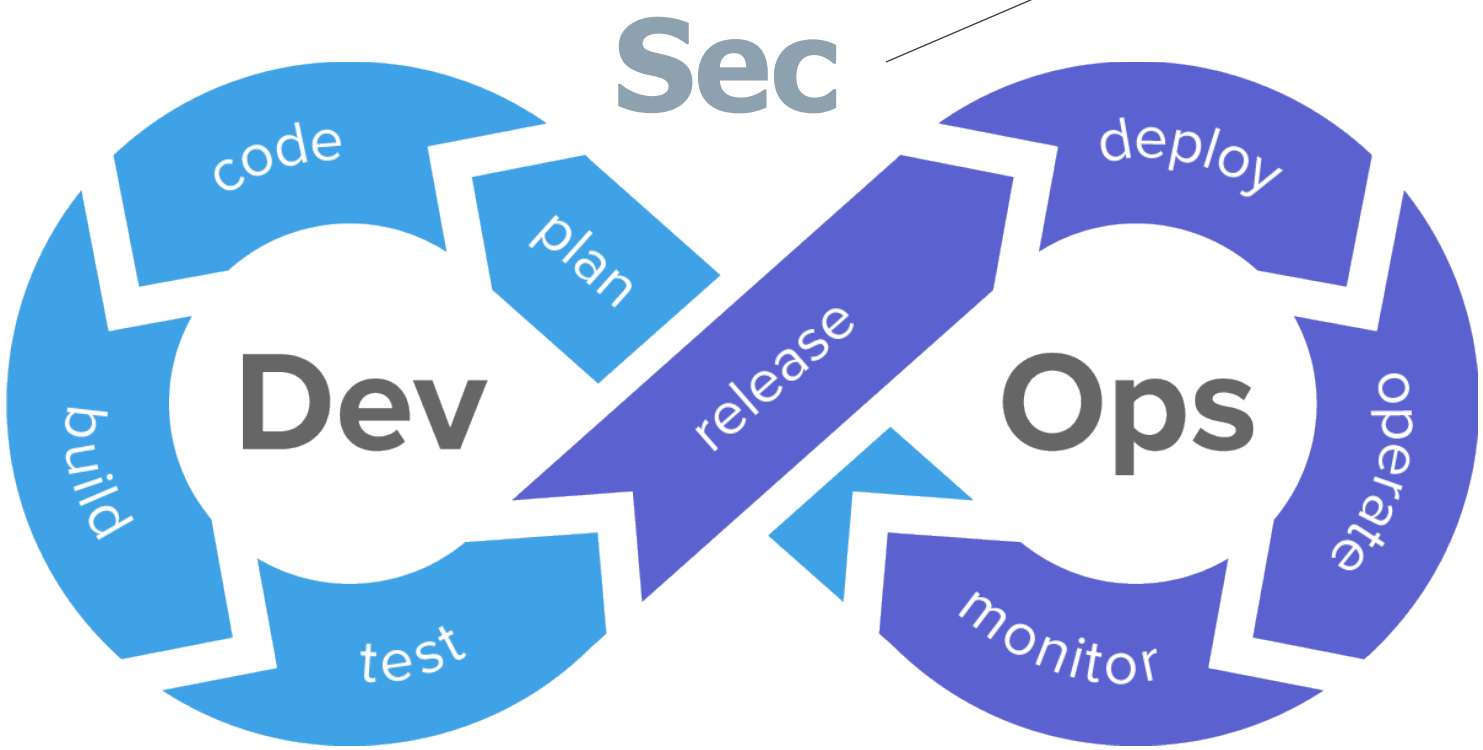
Эволюция бизнеса

Пять предвестников эволюции:

1. Цифровизация
2. Конкуренция бизнеса на уровне ИТ технологий
3. Рост кибер-преступности и снижение стоимости атак
4. Устаревание сигнатурных методов «Знай врага в лицо»
5. Пандемия и переход на удаленную работу



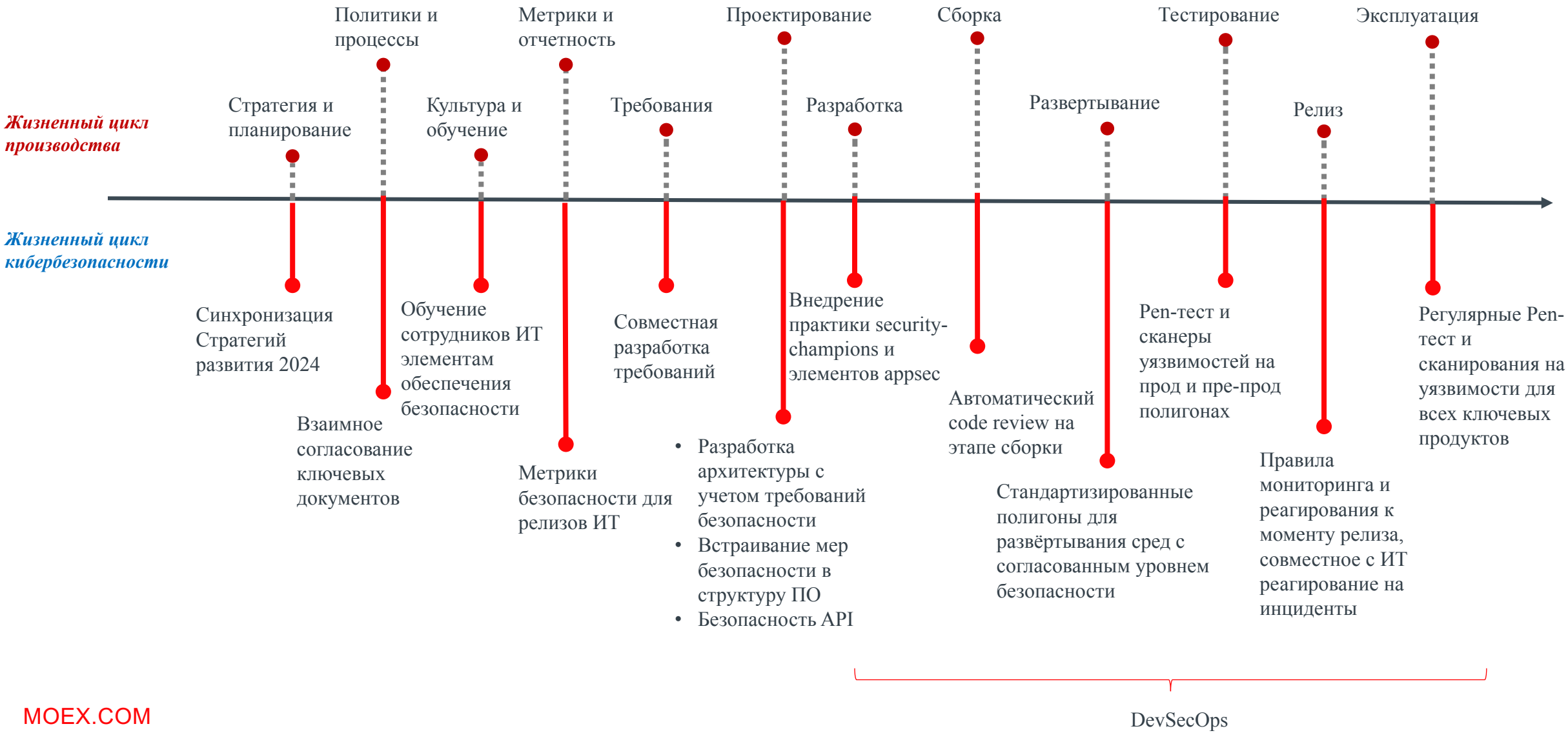
Сдвиг влево



- Security in Design
- Code Review
- Pen. Testing
- Repository control
- Security Monitoring
- App. Security
- Automated security testing
- Integrated security scanners
- Encrypt data between apps and services
- Secure API gateways
- Centralized user identity

Основа процессов безопасной разработки

Синхронизация стратегий ИТ и ИБ



Безопасная разработка

MOEX GROUP

Внешний контур – Интернет

- Артефакты/библиотеки разработки
- Open-source код из GitHub/GitLab
- Дистрибутивы ПО

Внутренний контур – MOEX

1 security gate	2 security gate	3 security gate
Полное закрытие контура MOEX	Локальная разработка	Разделение окружений производства
Проверка на уязвимости и лозунги	Запуск конвейера CI/CD	Проведение пентестов
Композиционный анализ	Проверка кода – SAST	Непрерывный мониторинг аномалий
Уведомление и обучение команд разработки	Проверка артефактов на уязвимости, DAST	Логирование аудит-логов
Перенос артефактов во внутренние репозитории	Создание безопасных CD-пакетов	Доп. проверки со стороны QA-инженеров

Участие ИБ от dev до prod

Полное сопровождение разработки командой DevOps-платформы

Кит 3. Какие проблемы пытается решить регулятор?

Повысить безопасность ПО

Повысить уровень цифровизации Финсектора

Решение: Заменить требования к готовому ПО на требования к процессу разработки

Требования к ПО

- 1.8. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить использование для осуществления финансовых операций прикладного программного обеспечения автоматизированных систем и приложений, распространяемых некредитными финансовыми организациями своим клиентам для совершения действий в целях осуществления финансовых операций, а также программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), прошедших сертификацию в системе сертификации Федеральной службы по техническому и экспортному контролю (далее - сертификация) или оценку соответствия по требованиям к оценочному уровню доверия (далее - ОУД) не ниже, чем ОУД 4, в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности", утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года N 1340-ст "Об утверждении национального стандарта" (М., ФГУП "Стандартинформ", 2014) (далее - ГОСТ Р ИСО/МЭК 15408-3-2013) (далее - оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений).

- …

- По решению некредитной финансовой организации оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений проводится самостоятельно или с привлечением проверяющей организации.

- …

При этом сертификация в системе сертификации ФСТЭК – тупиковый вариант:

- **Малое число** сертификационных лабораторий
- **Долгий срок** проведения сертификации (около 6-12 месяцев на 1 продукт)
- Любое изменение в ПО фактически **обнуляет** статус сертификации
- **Продуктовые циклы** финансовых организаций более динамичны

Как работает ГОСТ15408?

ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности

ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности

ПРОФИЛЬ ЗАЩИТЫ
прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций

1. Требования к ПО
2. Требования к мерам безопасности
3. **Требования к процессу разработки ПО**

32

Совместимым объектом оценки для настоящего ПЗ является прикладное программное обеспечение автоматизированных систем и приложений финансовых организаций, предназначенное для функционирования на средствах вычислительной техники общего назначения (автоматизированные рабочие места, серверы), а также на мобильных устройствах (ноутбуки, смартфоны, планшеты, телефоны и иные).

Обсуждаемые изменения (2024)

ГОСТ 56939 «Защита информации. Разработка безопасного ПО»

Процессная часть:
- Обучение
- Формирование требований
- Управление конфигурациями
- Управление архитектурой
- Моделирование угроз и поверхности атаки
- Управление уязвимостями

Практическая часть:
- Анализ кода
- Статический анализ
- Динамический анализ
- Конвейер поставки артефактов
- Хранение секретов
- Композиционный анализ
- Цепочки поставки
- Функциональное и нефункциональное тестирование

СПАСИБО
ЗА ВНИМАНИЕ

+7 (495) 363-32-32