



Association
of European
Businesses

AEB North-Western Regional Committee

“Financial outlook 2018 - update for successful business”

15 February, 2018

***St. Petersburg,
Consulate General of Germany***

Ute Katzsch-Egli,

Deputy Consul General of Sweden in St. Petersburg

Opening Remarks

Andreas Bitzi,

Quality Partners

Chair of the AEB North-Western Regional Committee

Opening Remarks

Torsten Erdmann,

Commerzbank (Eurasija) AO

**Member of the Steering
Committee of the AEB North-
Western Regional Committee**

Opening Remarks

Tatiana Evdokimova,

Nordea Russia

Russian macro update

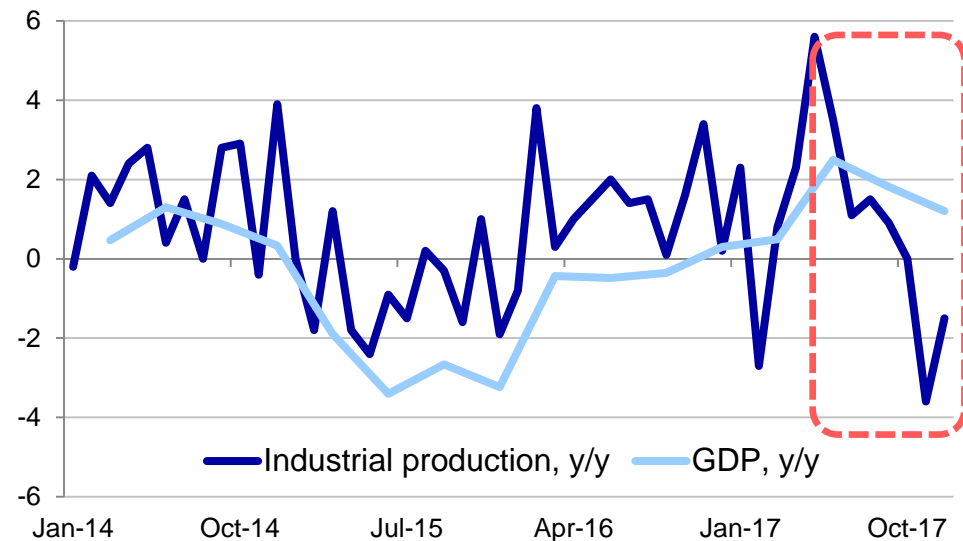
Tatiana Evdokimova
Chief Economist Russia

February 2018



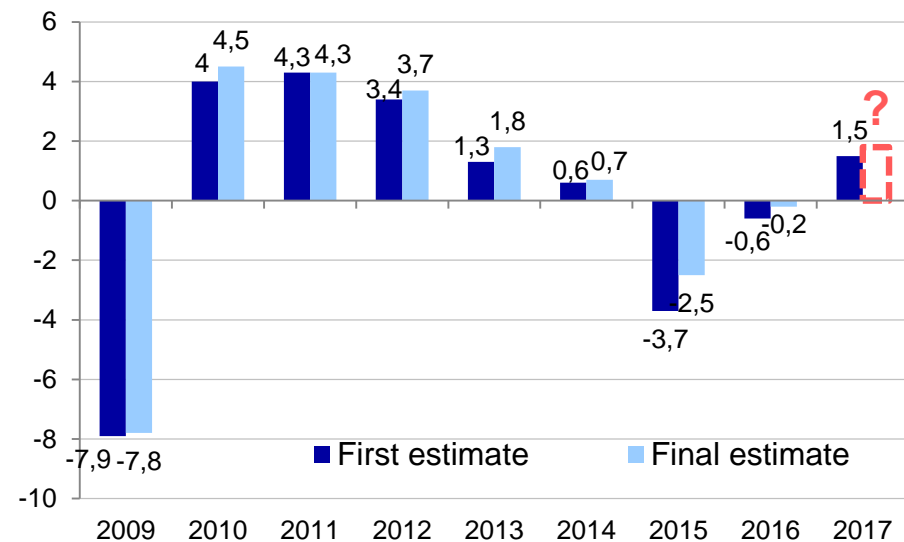
Macro data surprised on the downside at the end of 2017, however, it may yet be revised upward

Key economic indicators turned south in Q4 2017



Source: Nordea

Preliminary GDP figures usually underestimate actual growth



Source: Nordea

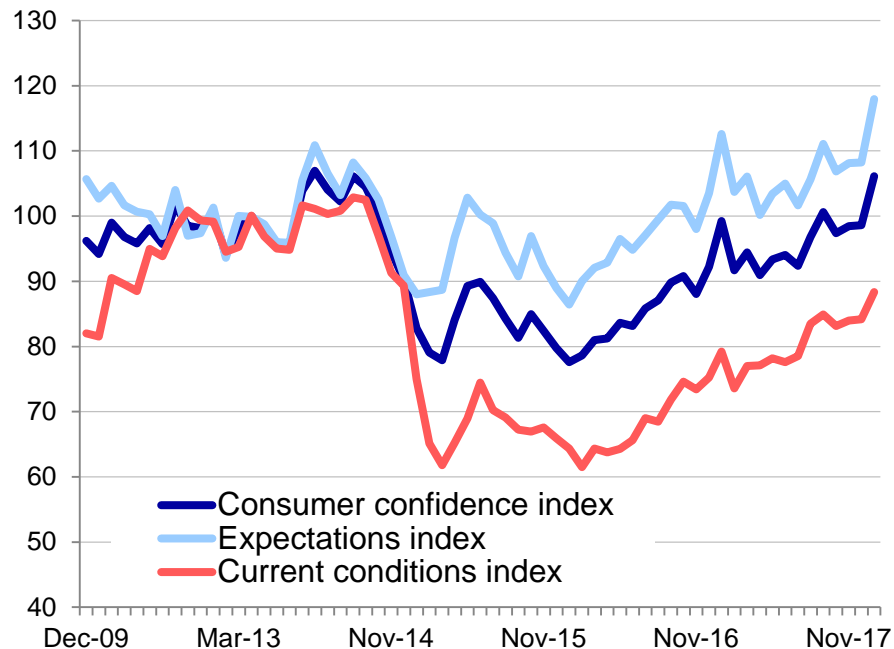
We still expect economy to accelerate in 2018 despite negative surprises of the end of 2017

	2017	2018	2019
GDP growth (real)	1,5	1,8	2,2
Export growth (vol)	5,4	3	2,5
Import growth (vol)	17	8	6
Retail sales	1,2	3	2,5
Government consumption growth	-0,9	0,6	0,5
Private fixed investment growth	3,6	2	3,5
Credit growth households	13,2	15	16
Credit growth enterprises	3,7	8,1	9,1
Unemployment (annual rate)	5,1	5	5
Wage growth	3,4	2,5	2

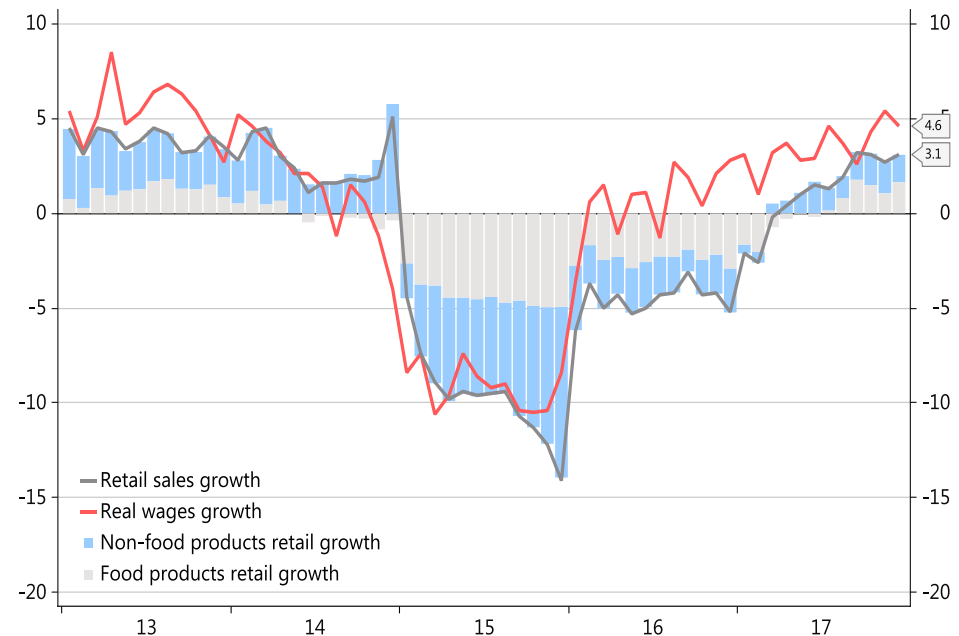
Source: Nordea Bank

Improving consumer confidence promises a strong start for retail this year

Consumer confidence indicators climb above pre-crisis highs



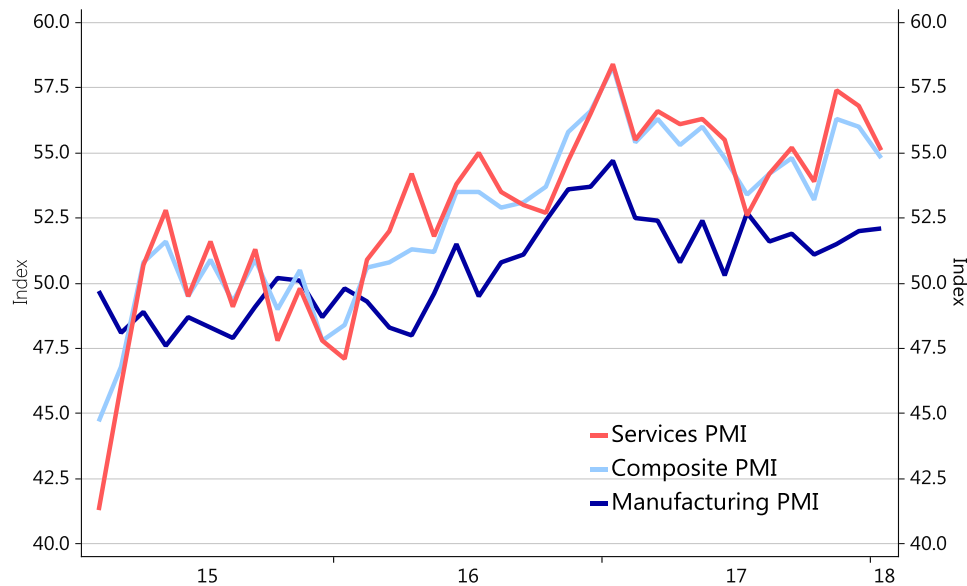
Tight correlation between retail sales and real wages comes back



Source: Nordea Markets and Macrobond

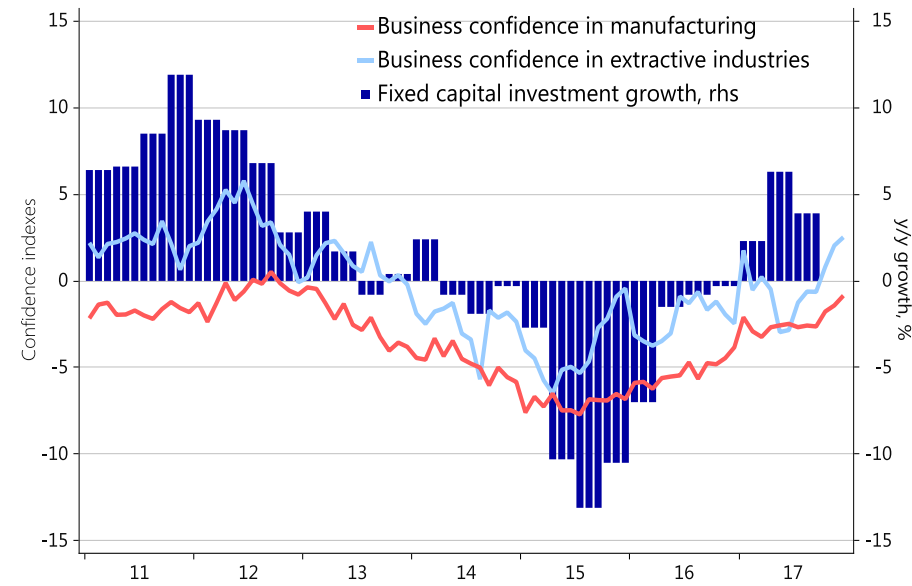
Leading indicators signal potential for further pick up in investment and industrial production

PMI remains above 50 for quite a while



Source: Nordea Markets and Macrobond

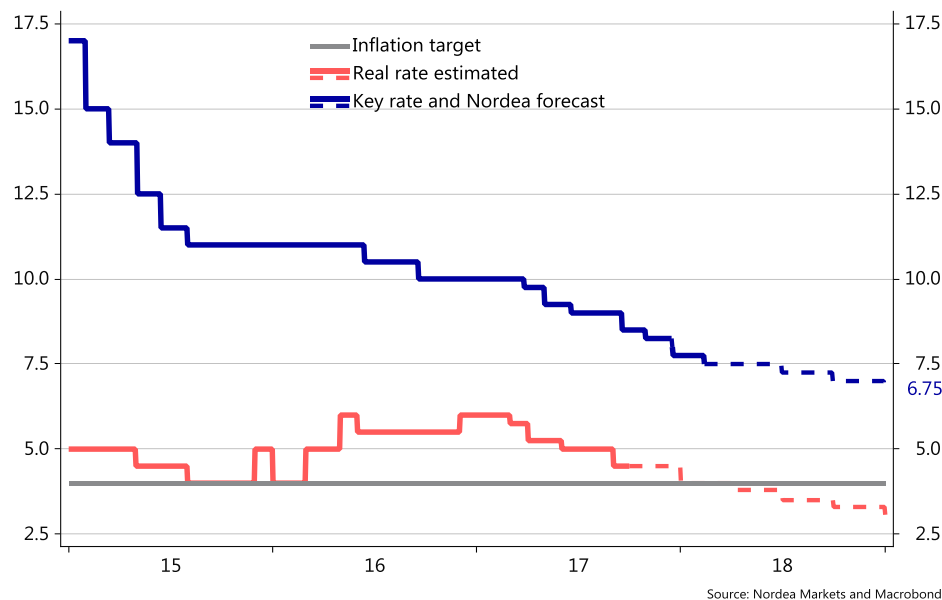
Business confidence recovering back to pre-crisis levels



Lähde: Nordea Markets ja Macrobond

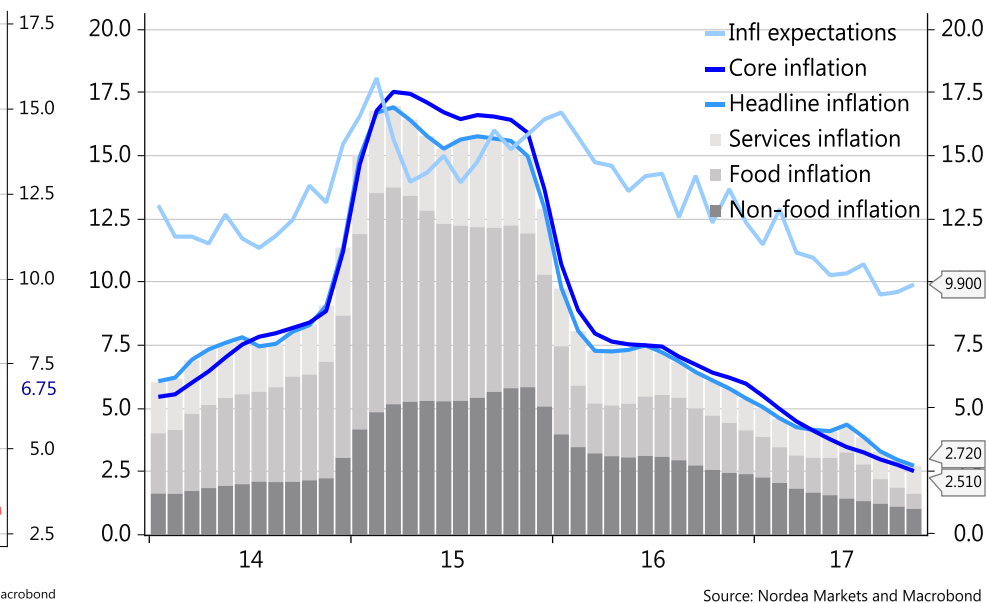
Key rate to decline further this year supporting recovery

The key rate is heading towards the medium term target of 6-7%



Source: Central Bank of Russia, Bloomberg

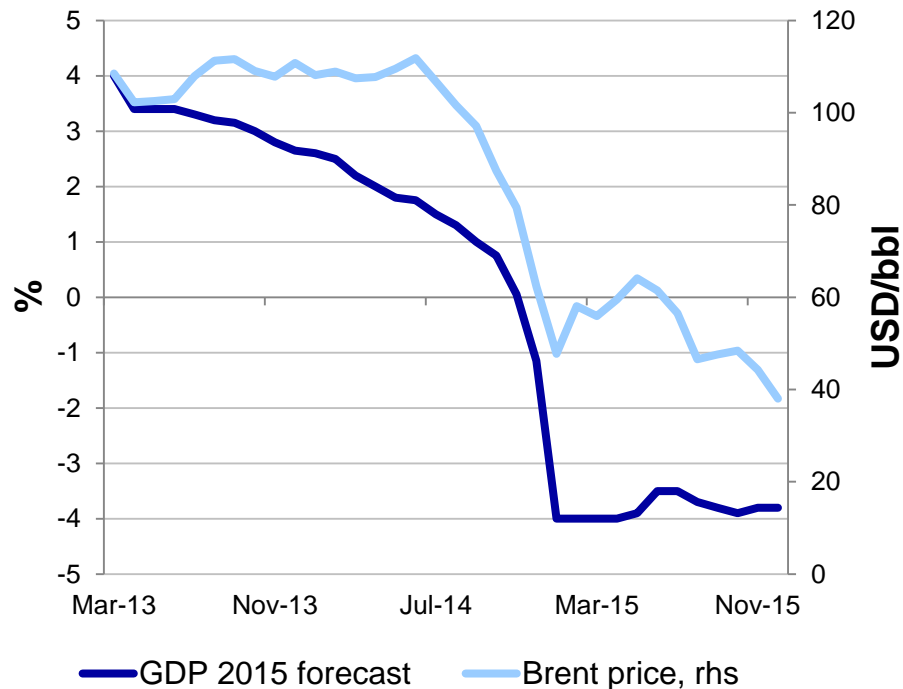
Still high inflation expectations limit the pace of monetary easing



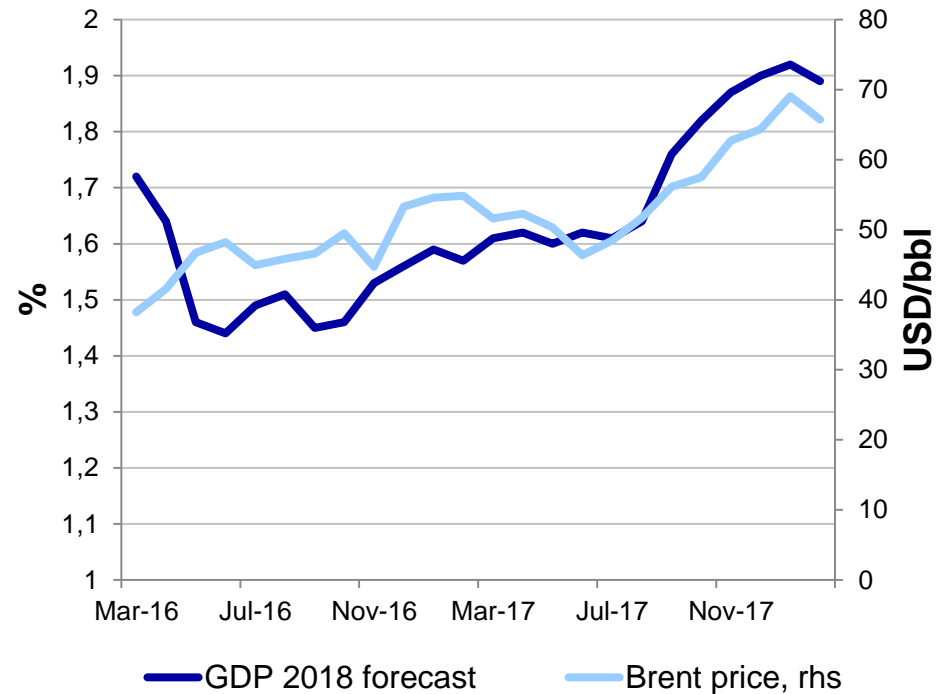
Source: Ministry of Finance

Oil price – still an important indicator for growth outlook

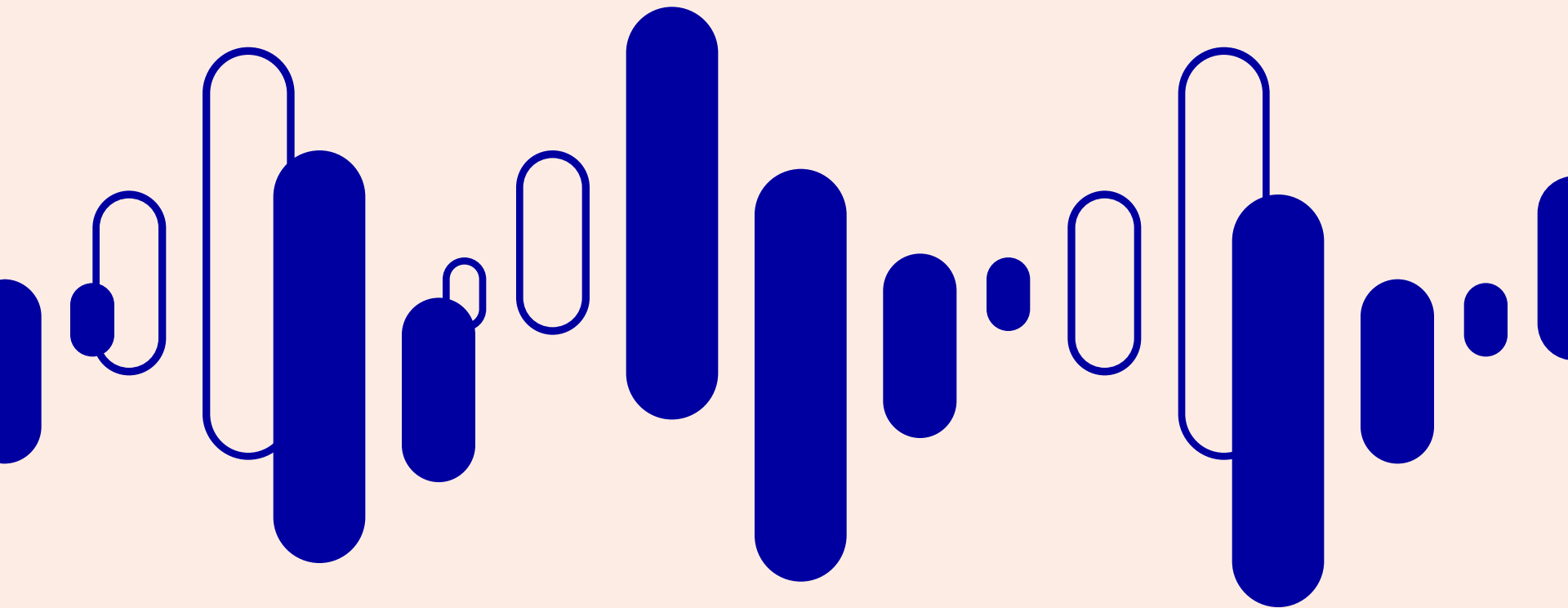
GDP growth forecasts for 2015 dropped sharply in 2014 following oil price dynamics



2018 growth outlook also mimics oil price dynamics

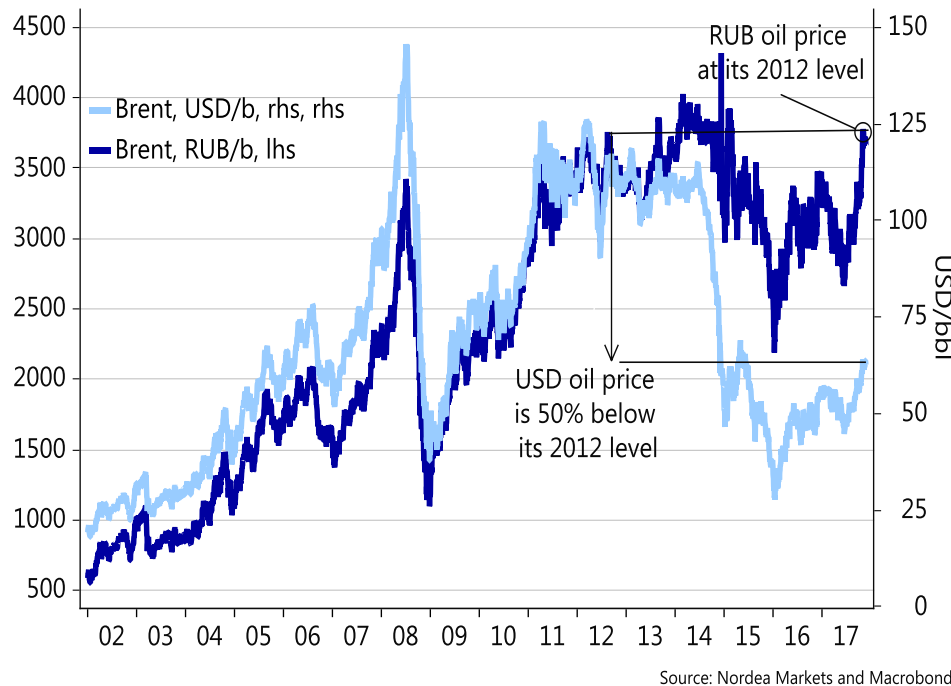


Higher resilience to external shocks



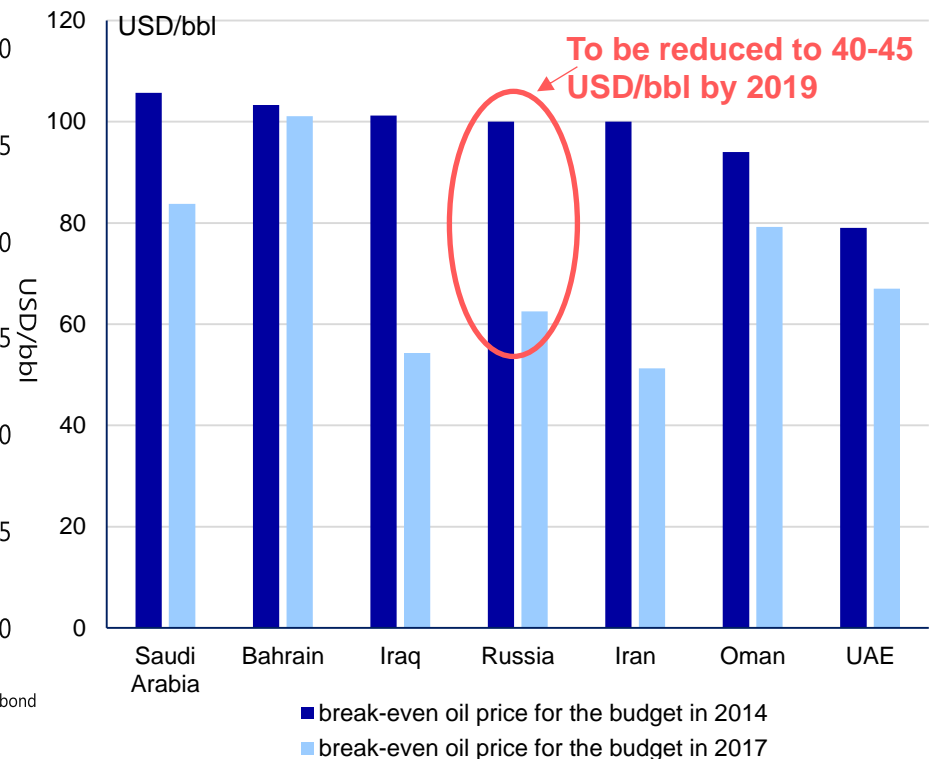
Budget policy to remain very conservative aiming at long term sustainability

Free floating RUB cushions oil price shocks for the budget



Source: Bloomberg

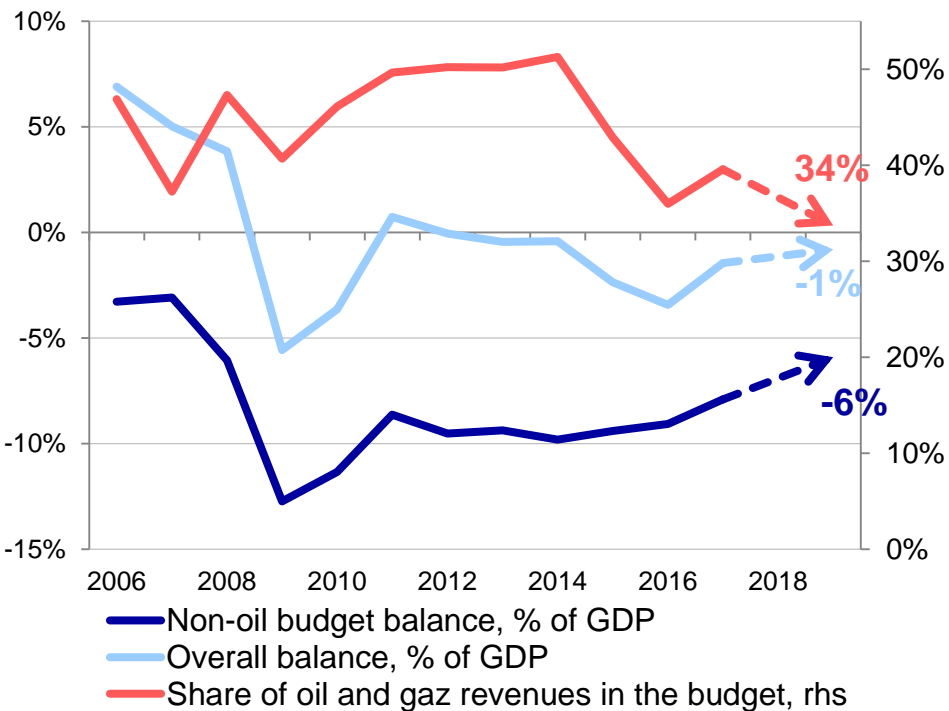
Russia is among countries that managed to adjust rapidly to the oil price shock



Source: IMF

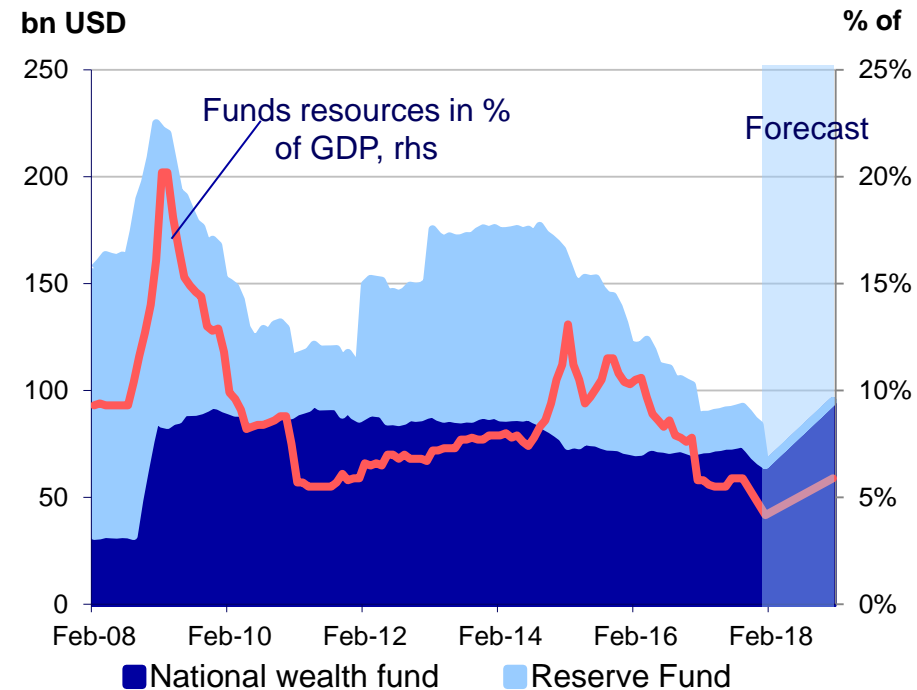
Government aims to reduce budget dependency on oil and to restart funds replenishment

The budget is already less dependent on oil and further improvement is planned for 2018-2019



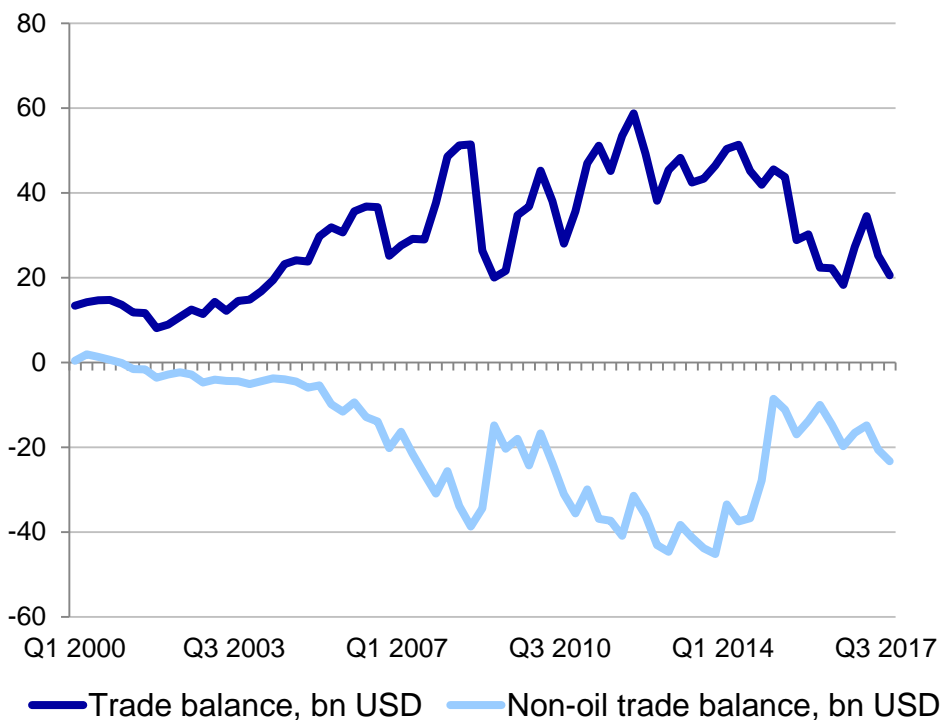
Source: Nordea

Minfin started replenishing sovereign funds in accordance with the new budget rule



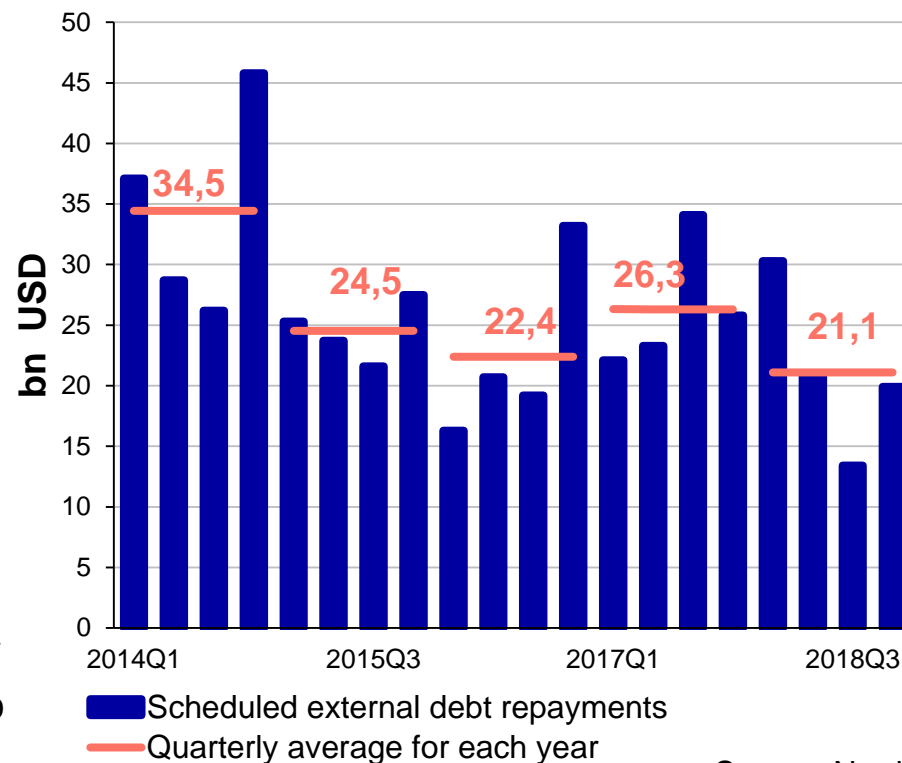
External account are getting more sustainable

External trade became more balanced on a non-oil basis



Source: Nordea

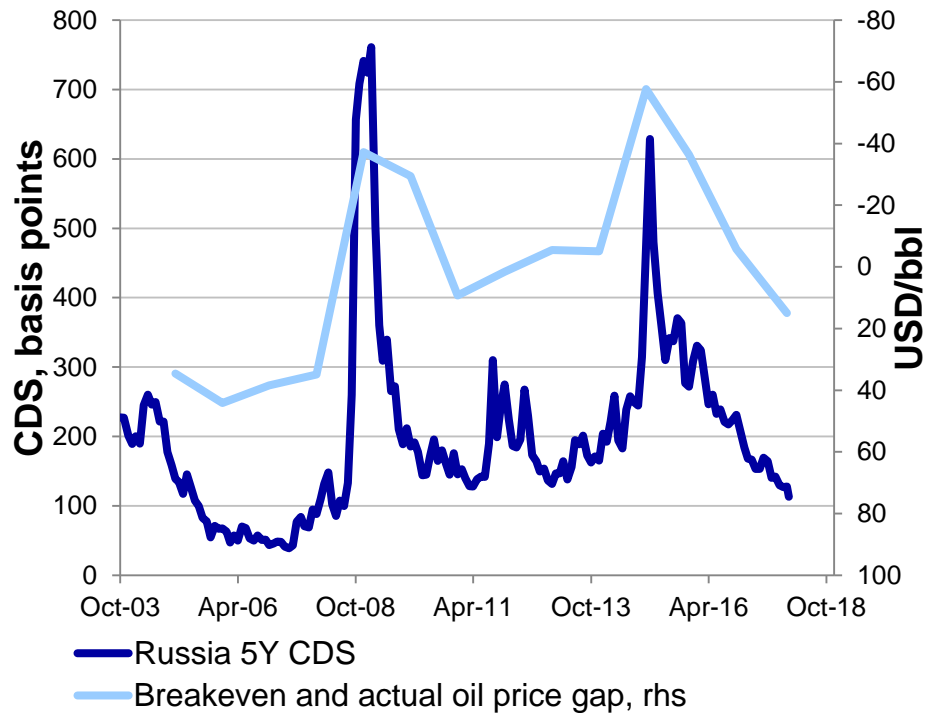
External debt service is getting easier



Source: Nordea

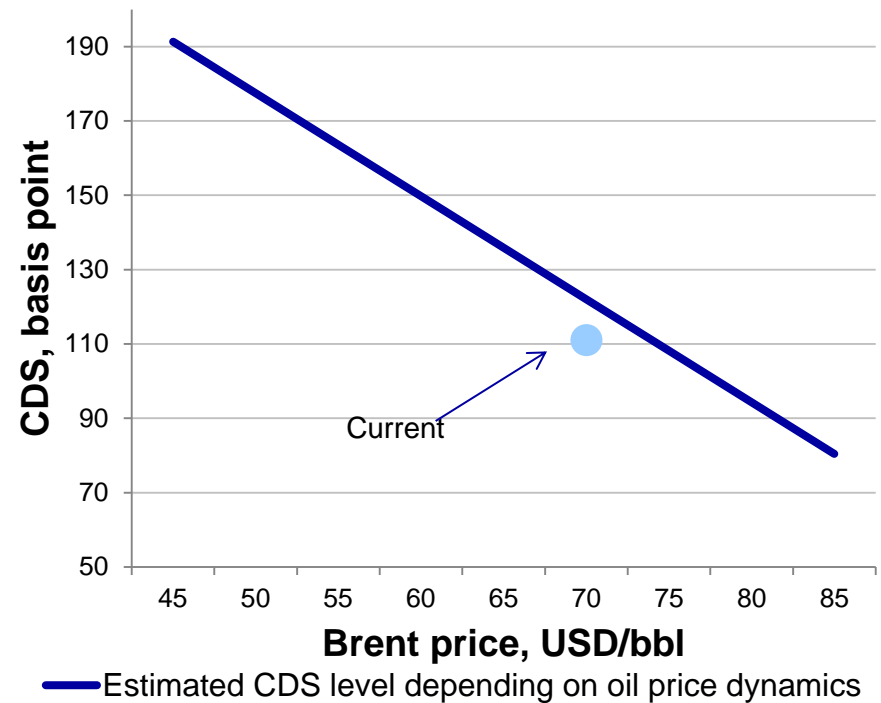
Markets are aware of Russia's improved macroeconomic fundamentals

Russian CDS vs the difference between breakeven and actual oil price



Source: Nordea

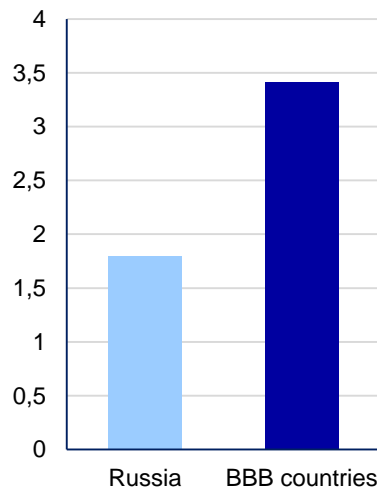
CDS sensitivity to oil prices assuming breakeven oil price of 45 USD/bbl



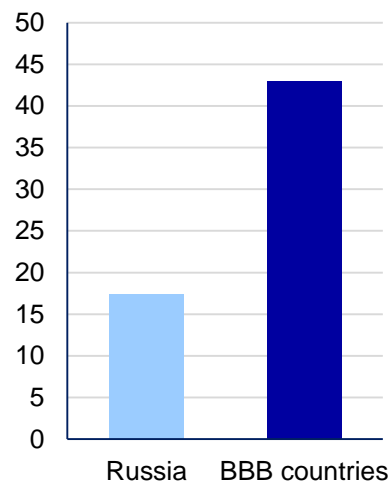
Source: Nordea

While rating agencies are lagging behind

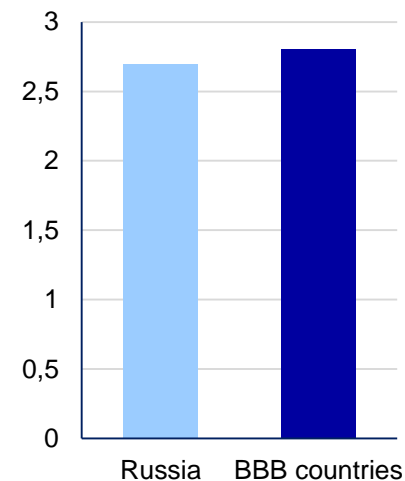
GDP growth



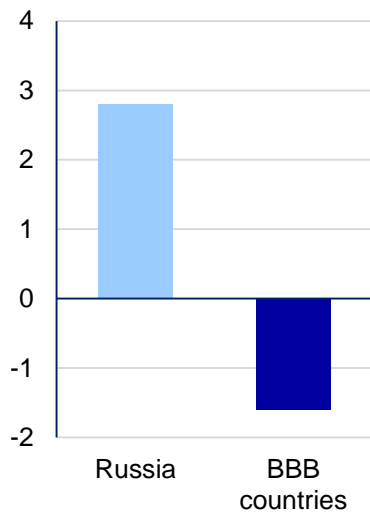
Public debt (% of GDP)



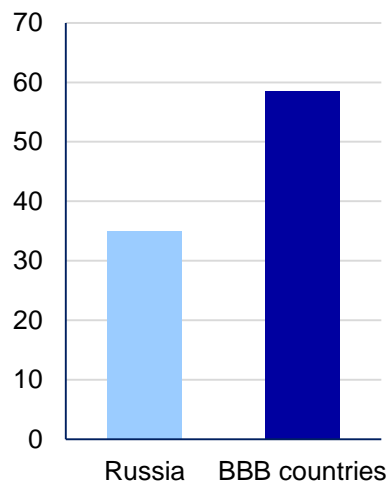
Inflation



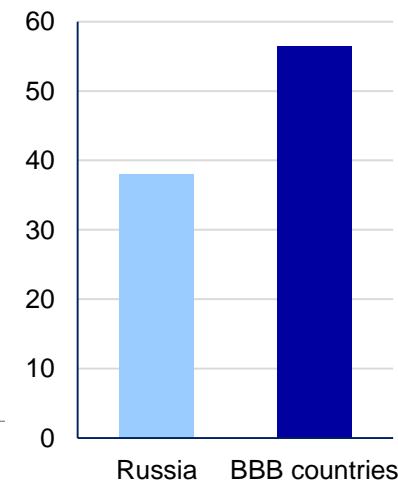
CA balance (% of GDP)



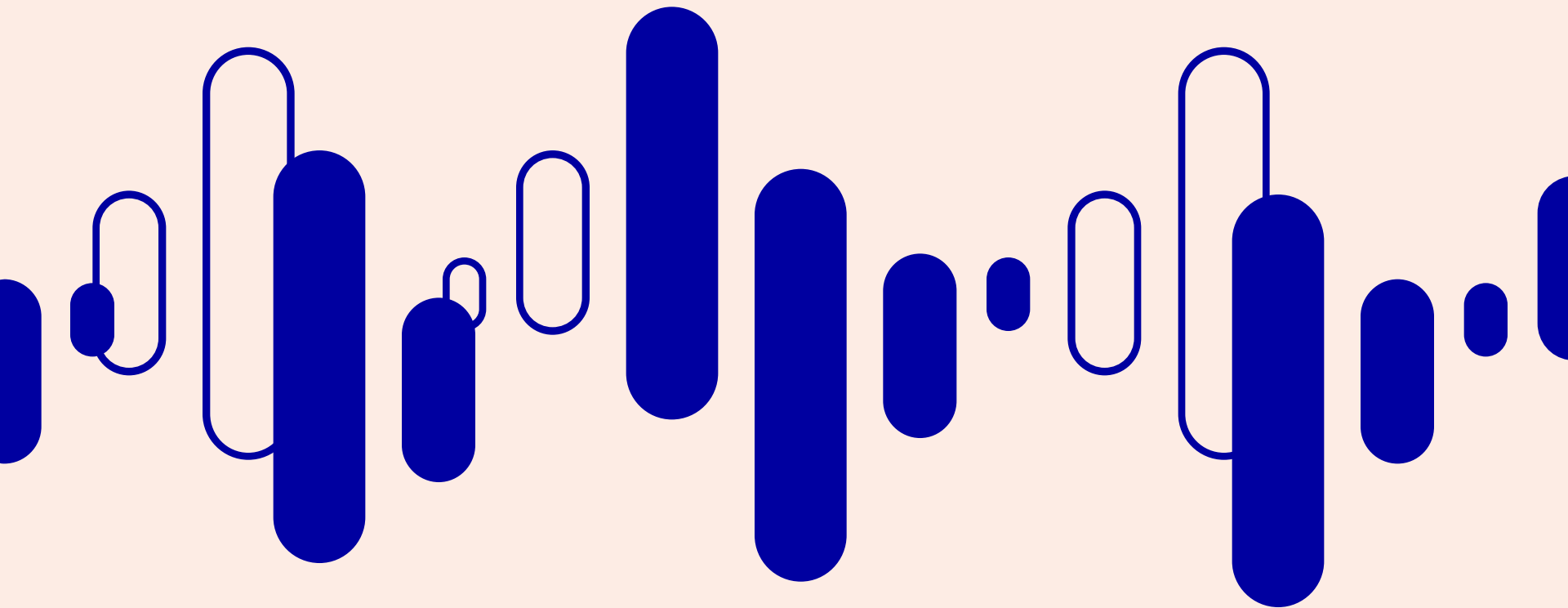
Doing business rank



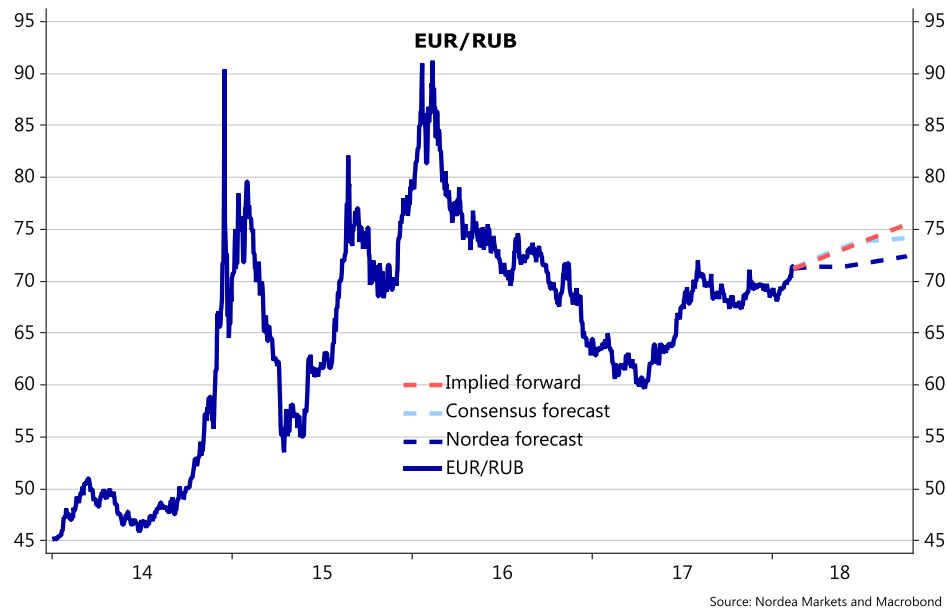
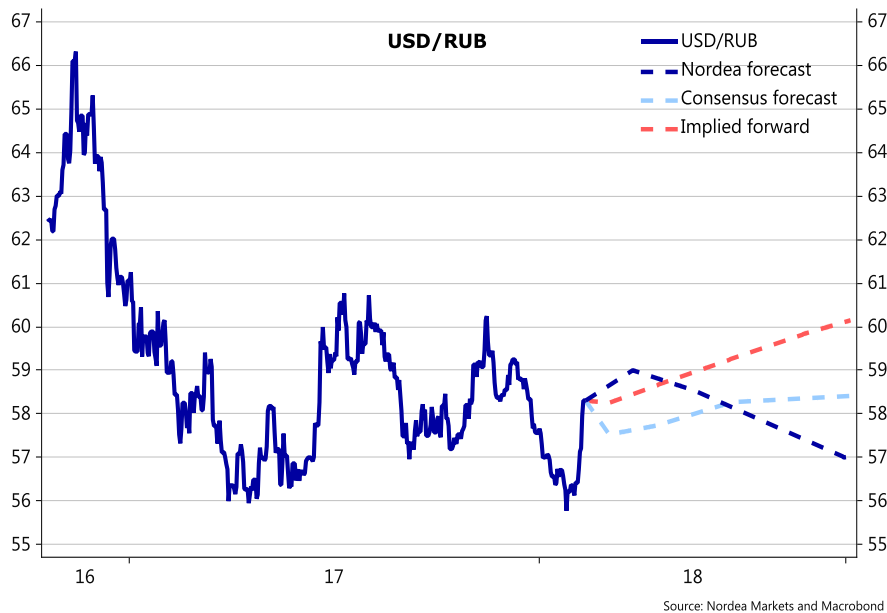
Competitiveness rank



RUB drifting away from being an oil-driven currency



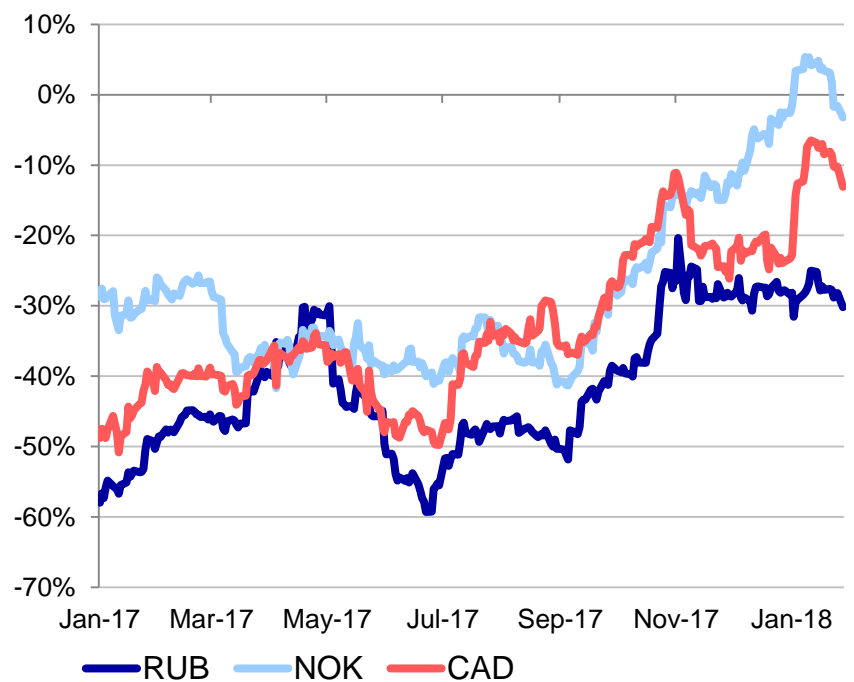
RUB forecast: short-term blurry, long-term glory



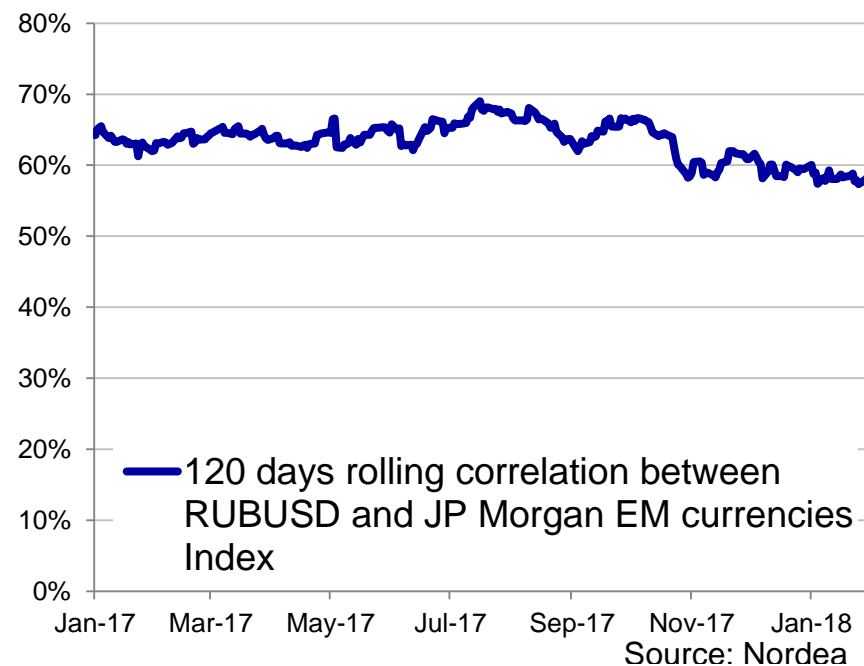
	Spot	3M	Mid-18	End-18	End-19
USDRUB	57,6	59	58,5	57	58
EURRUB	70,7	71,4	71,4	72,4	77,14

RUB is more and more a follower of general EM trends

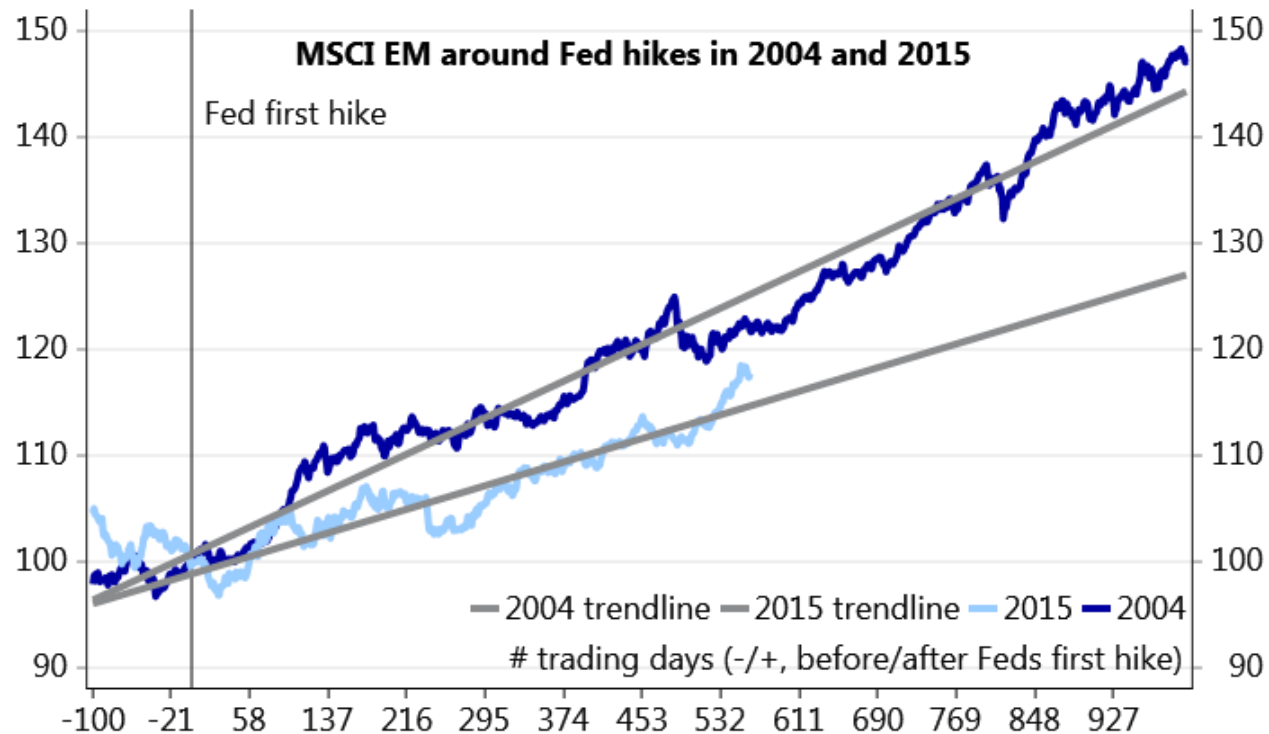
RUB correlation with oil decreasing in line with other oil-driven currencies trends



While general EM currencies trends represent the most important factor behind RUB dynamics



MSCI EM Currency Index likely to give away some of the recent gains



Source: Nordea Markets and Macrobond

Thank you!

Nordea Markets is the name of the Markets departments of Nordea Bank AB (publ), including its head office in Sweden, the branches in Denmark, Norway, Finland and Nordea Bank JSC (Russia).

The information provided herein is intended for background information only and for the sole use of the intended recipient. The views and other information provided herein are the current views of Nordea Markets as of the date of this document and are subject to change without notice. This notice is not an exhaustive description of the described product or the risks related to it, and it should not be relied on as such, nor is it a substitute for the judgement of the recipient.

The information provided herein is not intended to constitute and does not constitute investment advice nor is the information intended as an offer or solicitation for the purchase or sale of any financial instrument. The information contained herein has no regard to the specific investment objectives, the financial situation or particular needs of any particular recipient. Relevant and specific professional advice should always be obtained before making any investment or credit decision. It is important to note that past performance is not indicative of future results.

Before making any investment or credit decisions in all cases it is recommended to obtain professional advice. This presentation is not such advice. Any results and indicators of previous years are not guarantees of similar results and performance in future. Transactions in financial instruments may involve significant loss risks. Nordea Markets is not responsible for any losses.

Nordea Markets is not and does not purport to be an adviser as to legal, taxation, accounting or regulatory matters in any jurisdiction. Relevant professional advice should always be obtained before making any investment or credit decision.

This document may not be reproduced, distributed or published for any purpose without the prior written consent from Nordea Markets.



Association
of European
Businesses

Natalia Maygova,

SEB Russia



Association
of European
Businesses

COFFEE-BREAK

Ivan Yakimenko,

Commerzbank (Eurasija) AO

COMMERZBANK



Актуальные угрозы информационной безопасности платёжных систем банка

АО «Коммерцбанка (Евразия)» | IT department Moscow | Якименко Иван | Санкт-Петербург 2018

Кибератаки на различные отрасли в РФ


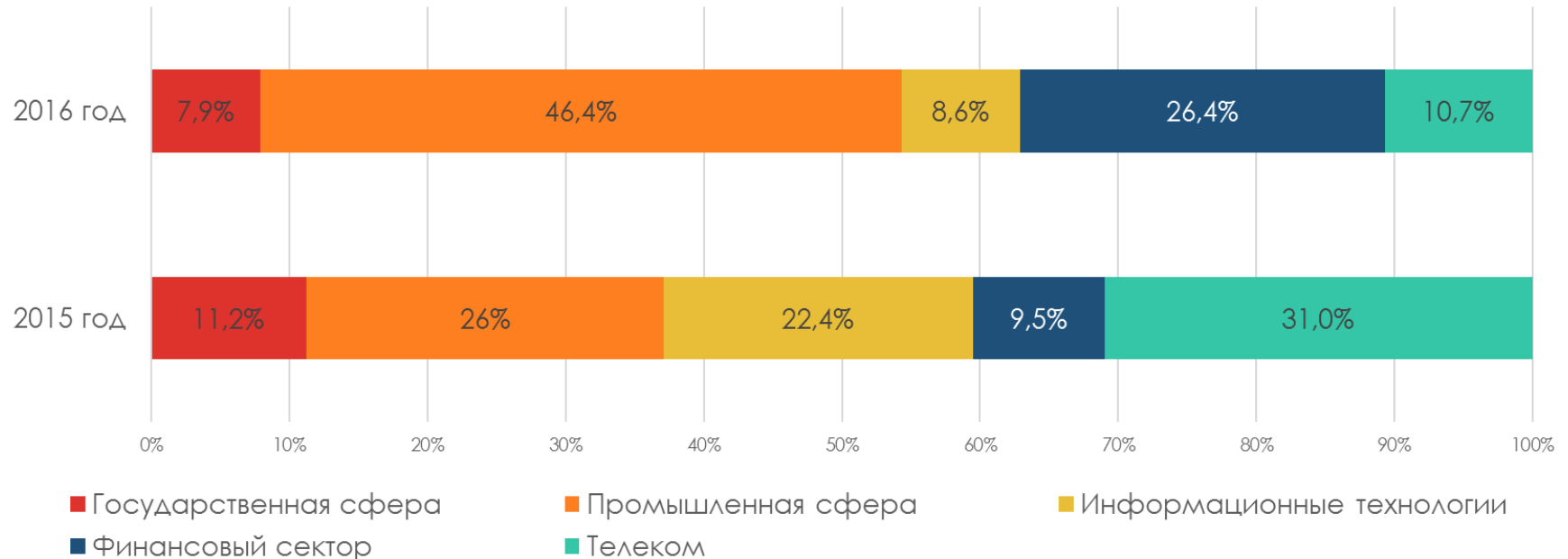


«Большинство российских компаний не могут успешно противостоять кибератакам, говорится в исследовании международной консалтинговой компании PwC, выпущенном в ноябре 2017 года»



По данным глобального исследования PwC Россия

Количество инцидентов информационной безопасности по отраслям



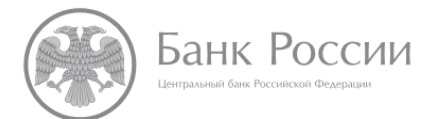
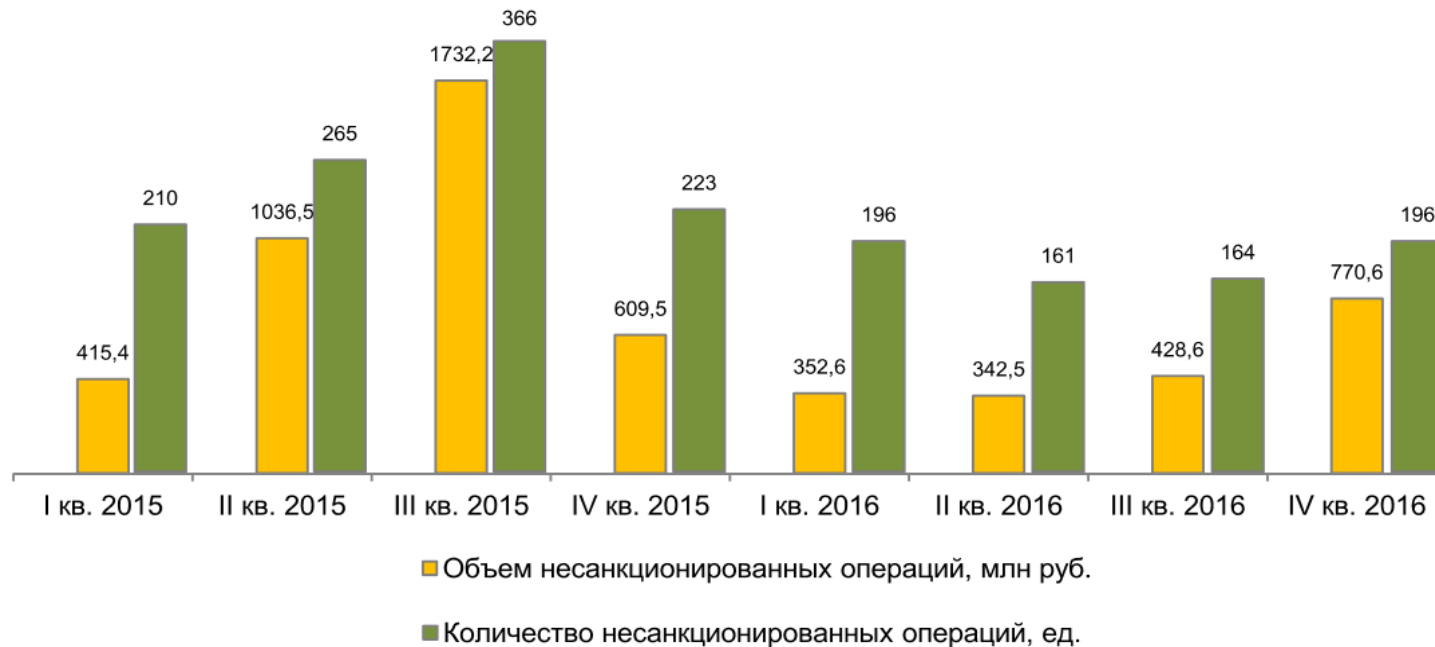
«В 2016 году Positive Technologies отметила новый всплеск компьютерных атак, направленных на организации финансовой сферы. Такие инциденты заняли более 26% от общего числа инцидентов, расследованных в 2016 году. Более того, в 2017 году прогнозируется 30-процентный рост числа сообщений об инцидентах в банках, процессинговых компаниях, брокерских компаниях, компаниях, занимающиеся денежными переводами, и финтехстартапах.»

*По данным расследований и обращений в компанию Positive Technologies

POSITIVE TECHNOLOGIES

Официальная статистика Центрального Банка РФ за 2015-2016

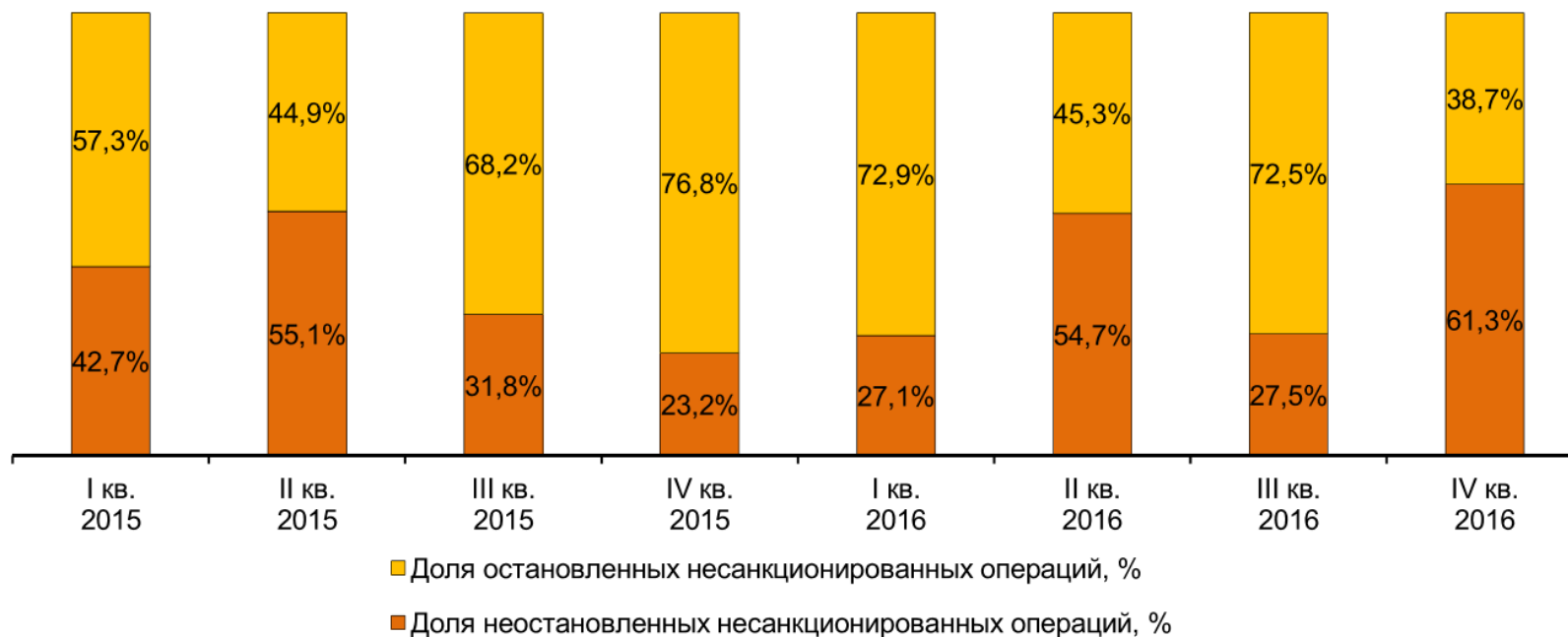
**Количество и объем несанкционированных операций
со счетов юридических лиц**



По данным официального отчета «Обзор несанкционированных переводов денежных средств за 2016 год» Центрального Банка РФ 2017

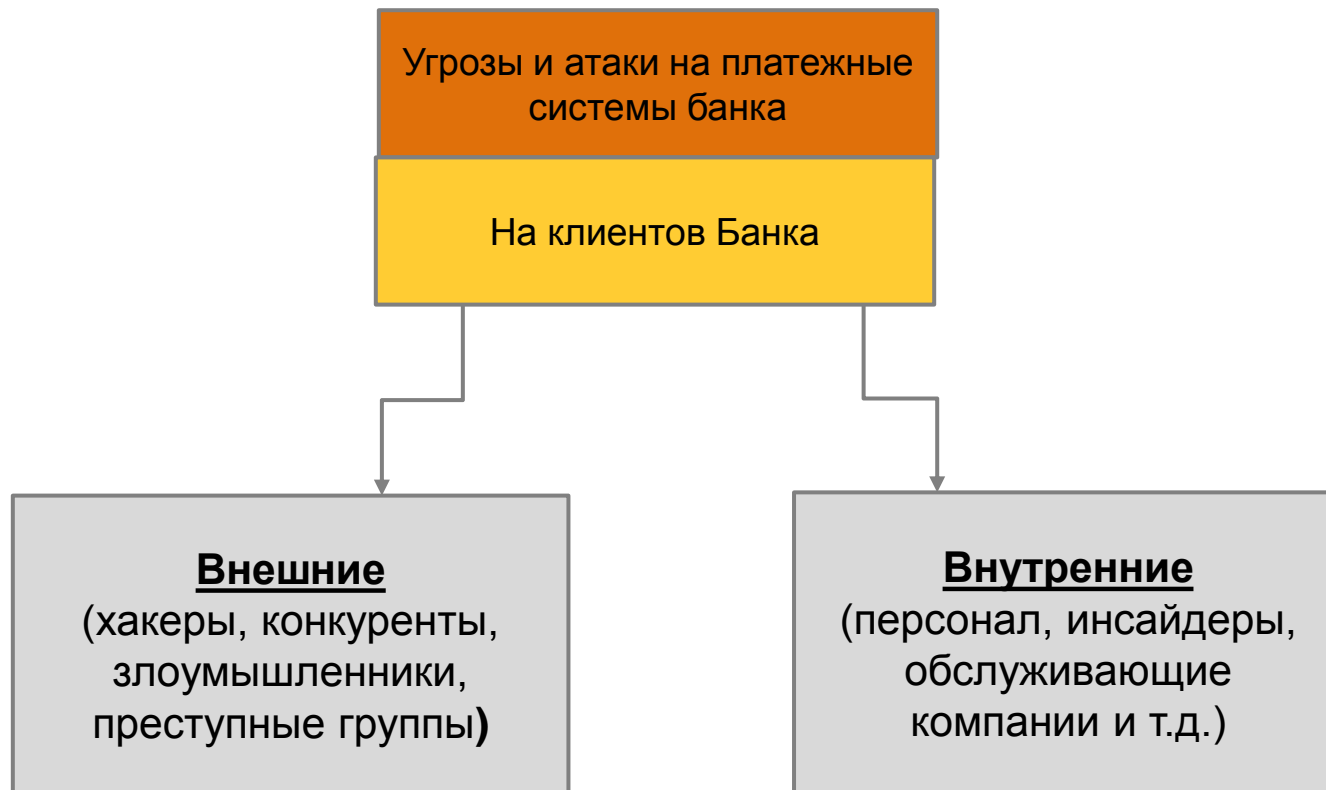
Официальная статистика Центрального Банка РФ за 2015-2017

Доля остановленных несанкционированных операций
со счетов юридических лиц



Законодательство РФ регулирующее работу платёжных систем банков и общие требования к защите информационных систем

- › ФЗ-161 «О Национальной платёжной системе» (закон гласит, что если клиент уведомляет банк о неправомерном использовании средств электронного платежа, банк обязан возместить ему сумму операции, совершённой без его согласия).
- › Положение Банка России № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств
- › Федеральный закон N 63-ФЗ "Об электронной подписи»
- › Федеральный закон N 149-ФЗ "Об информации, информационных технологиях и о защите информации"



Актуальные угрозы информационной безопасности для клиентов платежных систем банка, систем ДБО

1

Вредоносное ПО (трояны, вирусы, кейлогеры, клиенты бот-сетей и т.д.)

Наиболее распространённый способ атаки, заражения вирусами, троянами персонального компьютера клиента для получения информации и управления .

2

Социальная инженерия

Набирающий популярность метод получения необходимого доступа к информации, основанный на особенностях психологии людей и с применением технических средств.

3

Внутренние атаки инсайдеров, персонала

Собственные нелояльные сотрудники организации, пытающиеся получить конфиденциальные сведения или личную выгоду, шантаж работодателя;

4

Использование атак типа Man-in-the-Middle для проведения подложных транзакций;

вид атаки, когда злоумышленник тайно ретранслирует и, возможно, изменяет связь между двумя сторонами прошедших аутентификацию

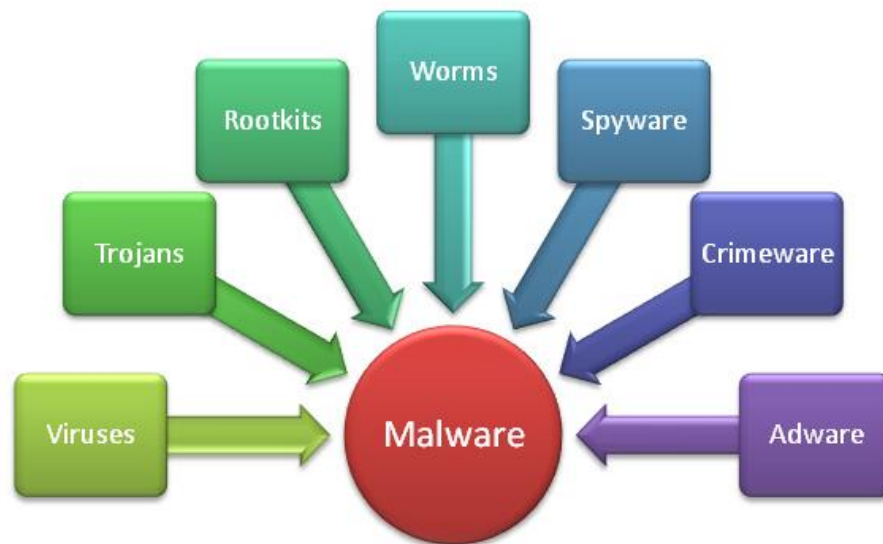
5

Использование уязвимостей ПО

Реализация заведомо известных уязвимостей в программном коде для получения контроля и данных системы.

Основные угрозы информационной безопасности для клиентов платежных систем банка, систем ДБО

Вредоносное ПО (трояны, вирусы, кейлогеры, клиенты бот-сетей и т.д.)

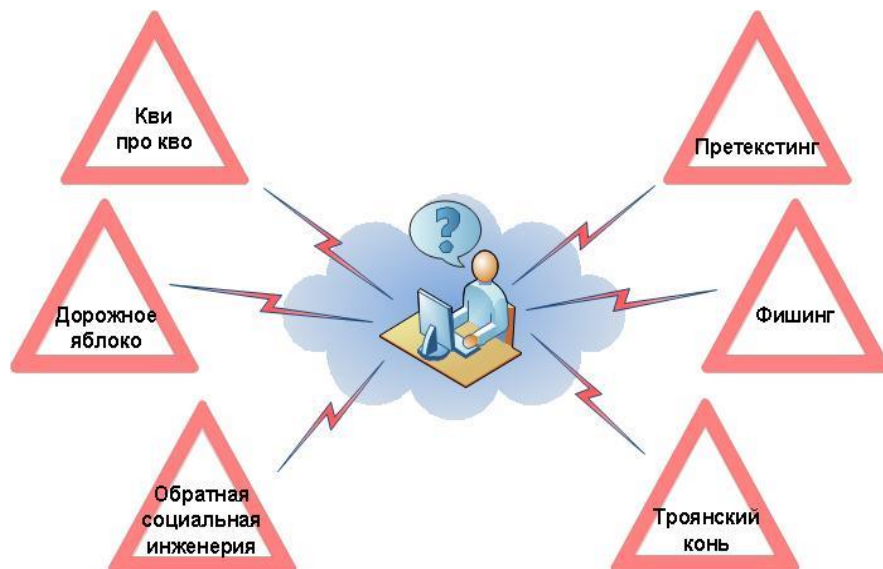


категории банковских троянов относятся вредоносные программы, предназначенные для похищения конфиденциальной информации и обеспечения несанкционированного доступа к системам дистанционного банковского обслуживания (ДБО). Многие банковские трояны сочетают в себе функции бэкдора и шпионских программ.

Наиболее распространенный метод проникновения банковских троянов в операционную систему, является их загрузка другими вредоносными программами - троянами-загрузчиками. Также большую опасность представляет возможность заражения при просмотре инфицированных веб-страниц — с использованием различных уязвимостей прикладного ПО. Помимо этого, банковские трояны могут проникнуть на компьютер жертвы в виде вложений в сообщения, массово рассылаемые по каналам электронной почты, на инфицированных съемных носителях, с использованием методов социальной инженерии.¹³

Основные угрозы информационной безопасности для клиентов платежных систем банка, систем ДБО

Социальная инженерия



Социальная инженерия - совокупность приёмов, методов и технологий создания такого пространства, условий и обстоятельств, которые максимально эффективно приводят к конкретному необходимому результату, с использованием социологии и психологии. Объектом атаки является человек и направлено на получение конфиденциальных данных (в случае платёжных систем – авторизационных данных)

Методы:

- Претекстинг
- Фишинг.
- Троянский конь
- Квид про кво (услуга за услугу)
- Дорожное яблоко
- Обратная социальная инженерия

Основные угрозы информационной безопасности для клиентов платежных систем банка, систем ДБО

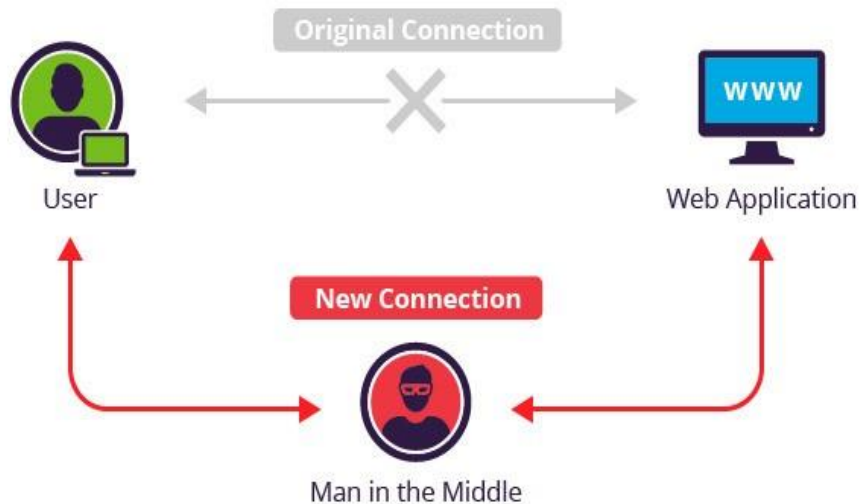
Внутренние атаки инсайдеров, персонала



Как правило нелояльные сотрудники являются достаточно распространённой угрозой платёжным системам банка. Неблагонадёжные родственные связи, обида на начальство, неоцененность, корыстные цели, сложные жизненные обстоятельства – основные причина, которые побуждают персонал организации клиента идти на мошенничество связанное с платёжными системами. Самое опасное и легко реализуемая угроза – когда персонал имеет непосредственно авторизационные данные и ключевые носители для работы с платёжной системой.

Основные угрозы информационной безопасности для клиентов платежных систем банка, систем ДБО

Использование атак типа Man-in-the-Middle для проведения подложных транзакций;



В рамках атак на платежные системы основной метод является внедрение кода для захвата уже авторизованной сессии, выполнения собственных команд на сервере и отправки ложных ответов клиенту.

Метод позволяет злоумышленнику вставлять свой код в электронные письма, SQL-выражения и веб-страницы (то есть позволяет осуществлять SQL-инъекции, HTML/script-инъекции или XSS-атаки), и даже модифицировать загружаемые пользователем бинарные файлы для того, чтобы получить доступ к учетной записи пользователя или изменить поведение программы, загруженной пользователем из интернета. Клиент на экране может видеть легитимные платёж, когда на сервер банка уходит платёж с изменёнными реквизитами

Основные угрозы информационной безопасности для клиентов платежных систем банка, систем ДБО

Использование уязвимостей ПО



Платежные системы представляют по сути приложения, состоящие из программного кода, для них характерны все уязвимости, известные в сфере безопасности приложений, а также угрозы, связанные со спецификой банковской сферы: хищение денежных средств, несанкционированный доступ к данным, к банковской тайне, отказ в обслуживании и другие угрозы, реализация которых может привести к существенным финансовым и репутационным потерям.

Наиболее часто встречаются уязвимости, позволяющие получить несанкционированный доступ к данным пользователей. К этой категории в основном относятся недостатки авторизации. Также — уязвимости связанные с «Недостаточная защита сессии» (некорректное завершение сессий пользователей, некорректная настройка параметров, возможность параллельной работы с несколькими сессиями для одного пользователя, отсутствие привязки сессии к IP-адресу клиента).

Основные причины возможности реализации угроз на стороне клиентов платежных систем банка, систем ДБО

- › Отсутствие полноценных служб «Информационной Безопасности» и «Отделов информационных систем»
- › Не обеспечена должным образом сетевая защита в компании, не настроены межсетевые экраны
- › Отсутствие разграничение прав пользователе на используемом персональном компьютере
- › Отсутствие Противовирусных программных средств
- › Не проводятся своевременные обновления операционной системы и программных продуктов
- › Бесконтрольный доступ к персональному носителю ключевой информации, нарушения правил хранения
- › Использование персонального компьютера для бесконтрольного «серфинга» в сети интернет
- › Очень слабая осведомлённость персонала в вопросах информационной безопасности
- › Передача аутентификационной информации и ключевых носителей третьим лицам

Примеры реализации угроз и атак

Распространённый вид смешанных атак

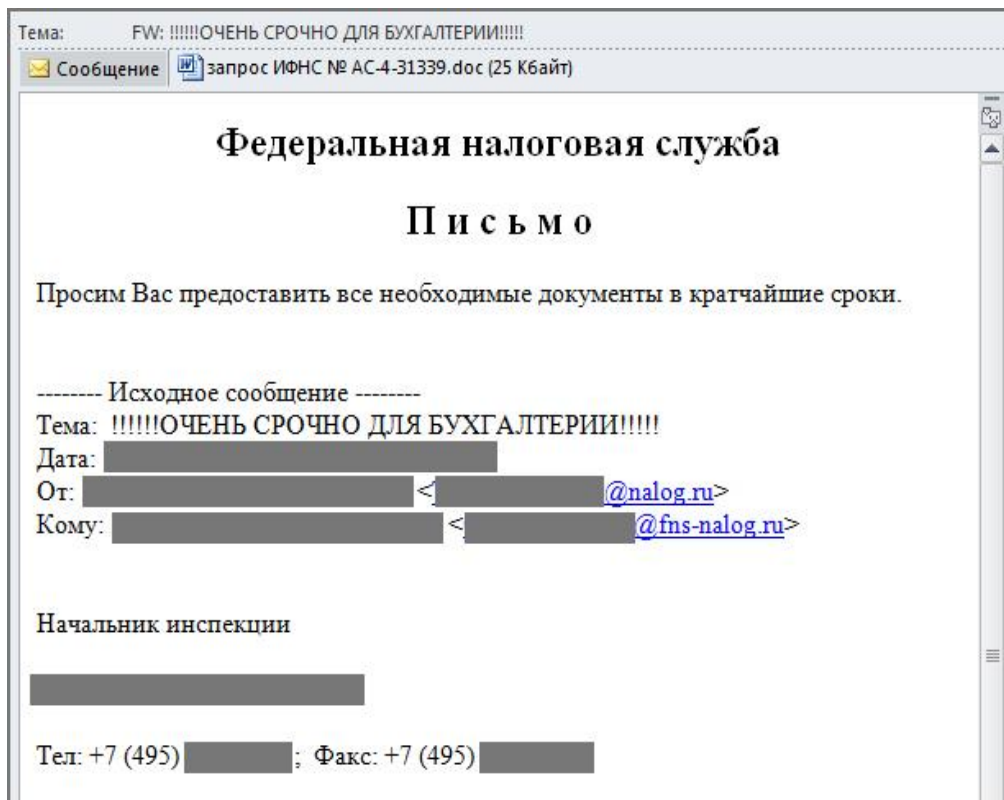


Схема атаки

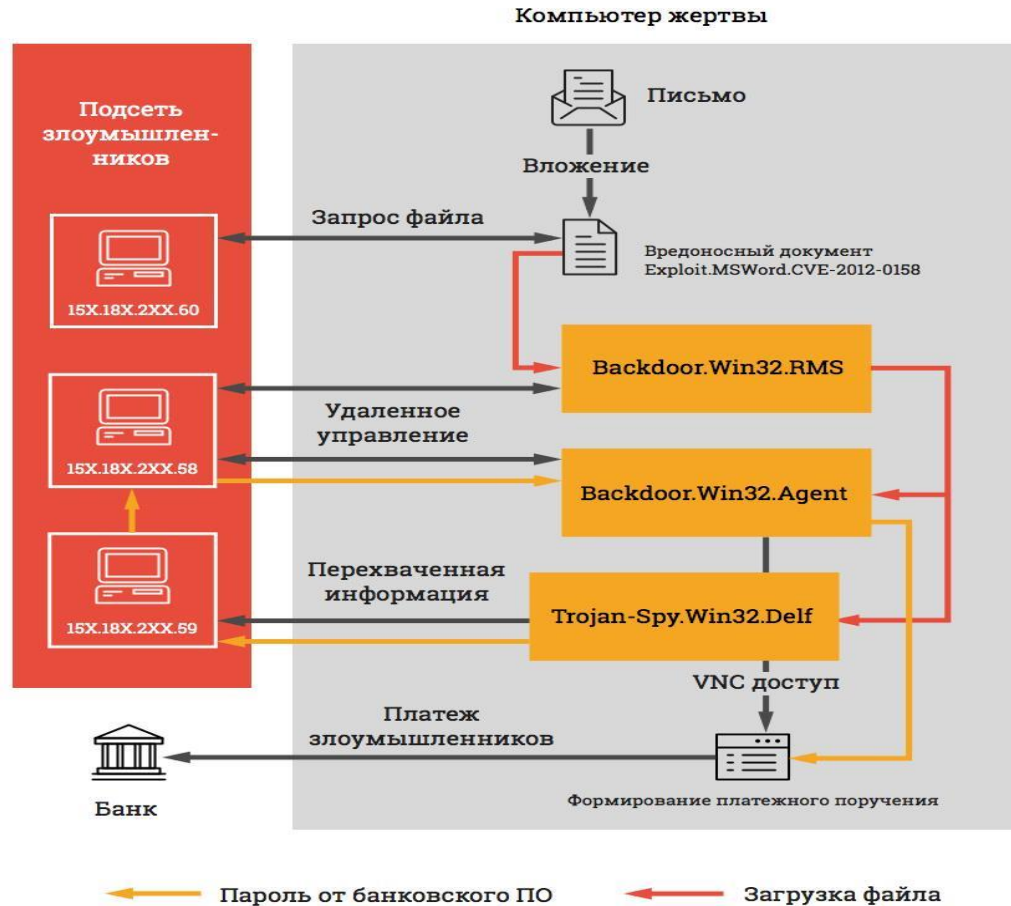
1. В ходе целевой атаки с использованием социальной инженерии и уязвимости в программе Microsoft Word компьютер бухгалтера был заражен Backdoor.Win32.RMS.
2. С помощью этого бэкдора злоумышленники загрузили на зараженную машину еще две вредоносные программы: кейлоггер (Trojan-Spy.Win32.Delf) и бэкдор (Backdoor.Win32.Agent), предоставляющий удаленный VNC доступ к компьютеру жертвы.
3. Кейлоггер перехватил пароль для доступа к системе ДБО.



По данным расследований реальных случаев хищений средств от «Лаборатории Касперского»

Примеры реализации угроз и атак

Распространённый вид смешанных атак



4. Пока бухгалтера не было на рабочем месте, злоумышленники с помощью Backdoor.Win32.Agent, используя VNC доступ к компьютеру, запустили от имени бухгалтера банковское ПО.
5. Используя перехваченный кейлоггером пароль, киберпреступники сформировали и отправили в банк платежное поручение на сумму около 300 тыс. руб.
6. Чуть позже было сформировано и отправлено в банк еще одно платежное поручение – приблизительно на 3 млн. руб.

Спасибо за внимание



Уточняющие вопросы вы можете задать по реквизитам ниже

Якименко Иван Александрович

Главный специалист Отдела Информационных Систем

Phone: +7 495 797 48 26

E-mail: Ivan.yakimenko@commerzbank.com

Адрес:

Москва, Кадашевская наб., 14/2

Phone: +7 495 797 48 00

E-mail: itmoscow@commerzbank.com

Disclaimer

IT Department

This presentation has been prepared and issued by Commerzbank AG. This publication is intended for professional and institutional customers.

Any information in this presentation is based on data obtained from sources considered to be reliable, but no representations or guarantees are made by the Commerzbank Group with regard to the accuracy of the data. The opinions and estimates contained herein constitute our best judgement at this date and time, and are subject to change without notice. This presentation is for information purposes, it is not intended to be and should not be construed as an offer or solicitation to acquire, or dispose of any of the securities or issues mentioned in this presentation.

Commerzbank AG and/or its subsidiaries and/or affiliates (herein described as the Commerzbank Group) may use the information in this presentation prior to its publication to its customers. The Commerzbank Group or its employees may also own or build positions or trade in any such securities, issues, and derivatives thereon and may also sell them whenever considered appropriate. The Commerzbank Group may also provide banking or other advisory services to interested parties.

The Commerzbank Group accepts no responsibility or liability whatsoever for any expense, loss or damages arising out of, or in any way connected with, the use of all or any part of this presentation.



Association
of European
Businesses

Anton Poddubny,

Dentons

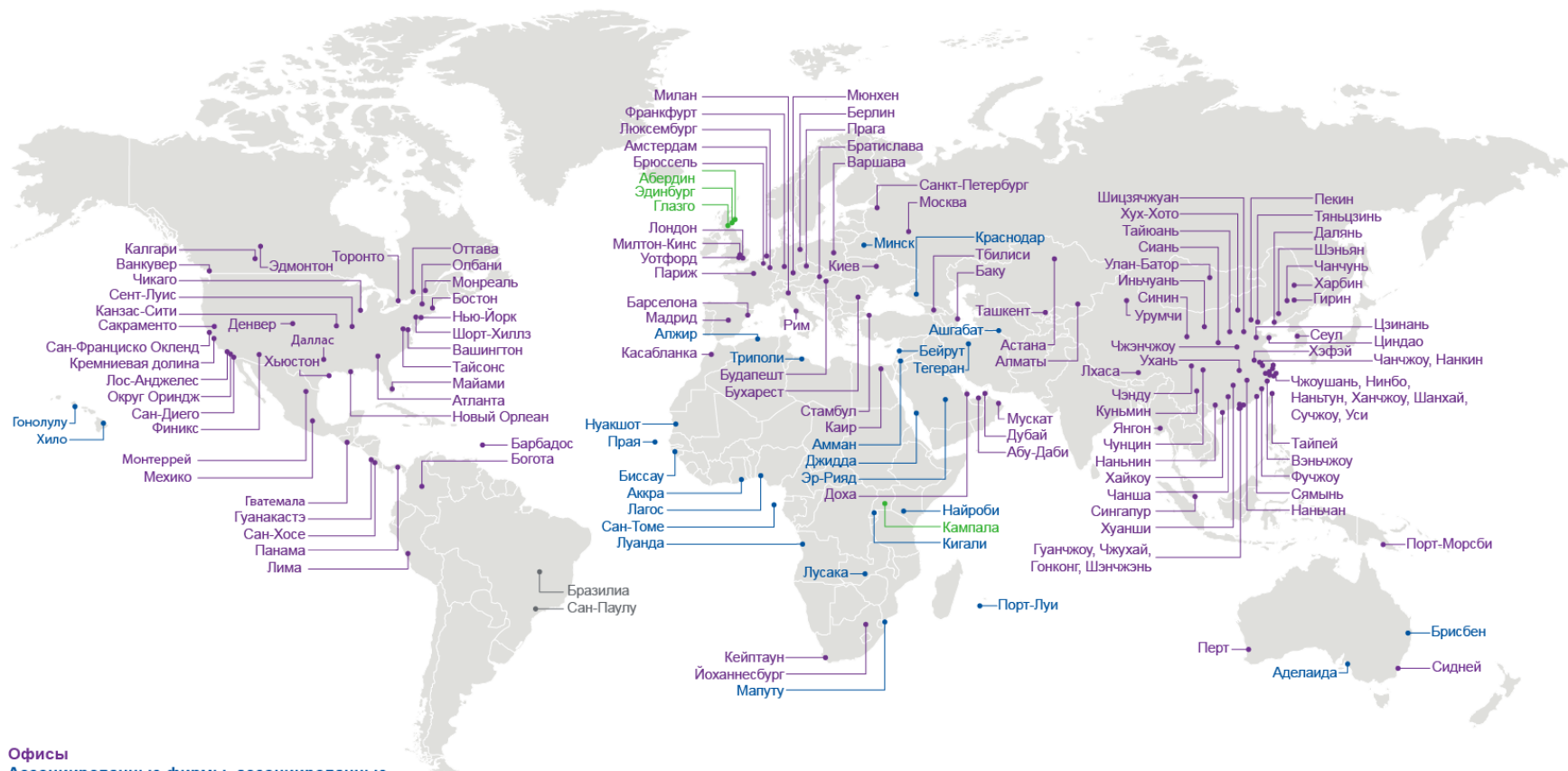
Финансовый обзор 2018. Новости для успешного бизнеса Криптовалюты. Правовой ландшафт и мировые тенденции

Антон Поддубный
Советник

15 февраля 2018 года



Dentons – самая крупная в мире юридическая фирма*



Офисы

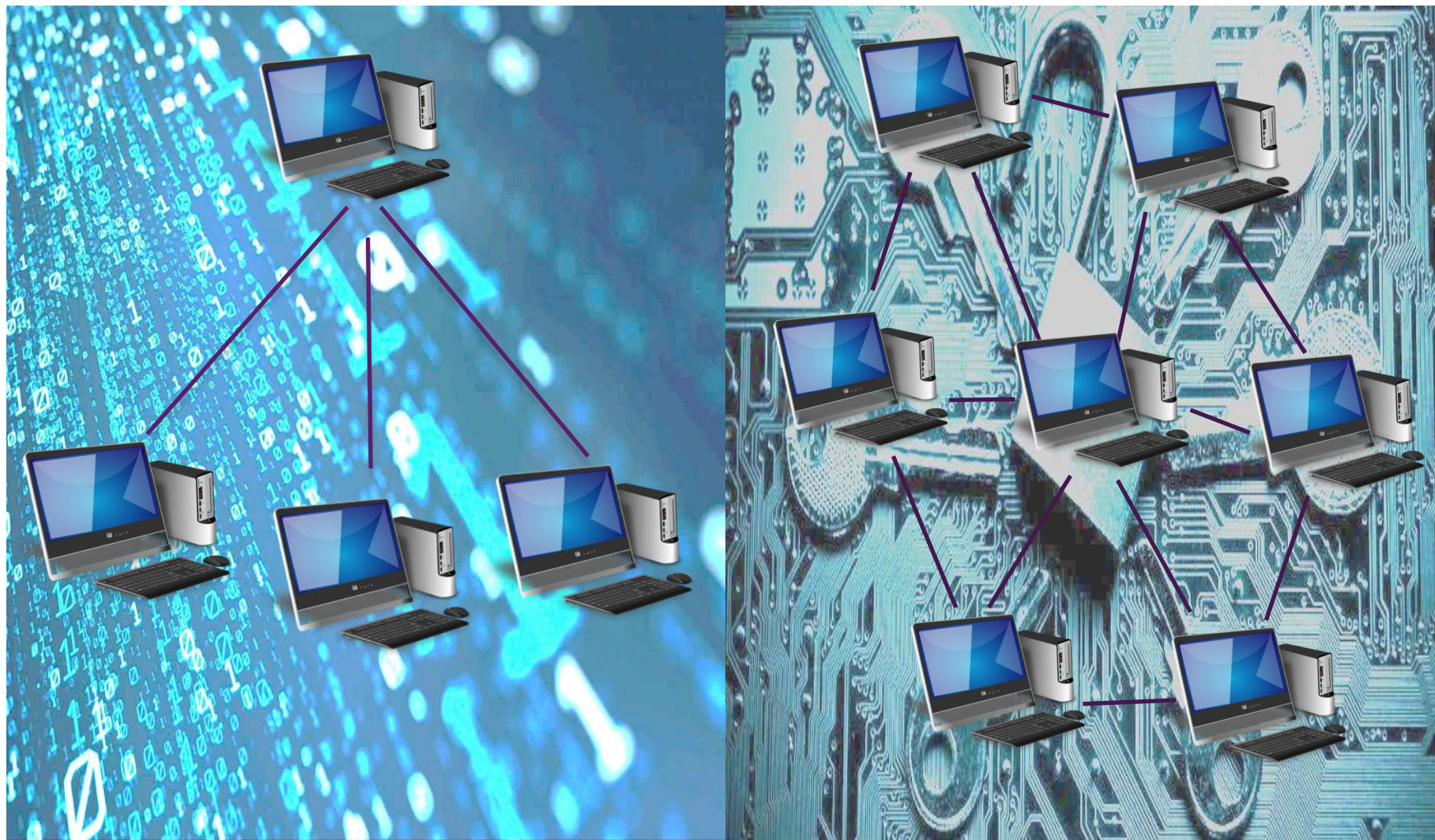
Ассоциированные фирмы, ассоциированные
офисы и фирмы - участники специальных альянсов

Офисы, отмеченные зеленым цветом, принадлежат тем
фирмам, с которыми Dentons находится в процессе объединения

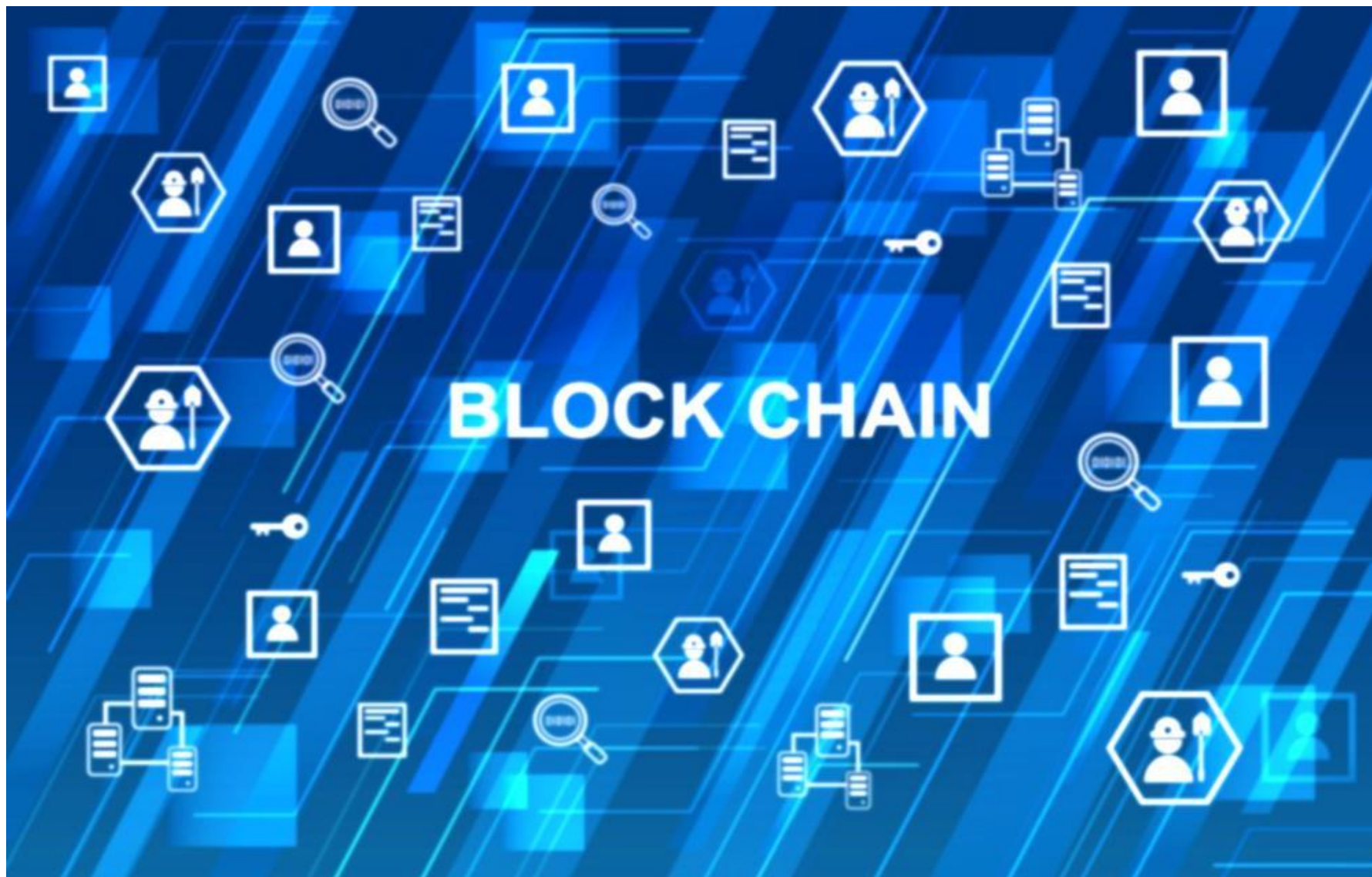
Офисы, отмеченные серым цветом, являются
участниками стратегических альянсов

* 2017 The American Lawyer – Рейтинг 100 международных юридических фирм по количеству юристов (Global 100).

Немного про блокчейн



Немного про блокчейн



A collage of various cryptocurrency logos and coins. In the center is a large orange circle with a white Bitcoin symbol. Surrounding it are numerous other coins and logos, including a silver coin with a panda (PandaCoin), a gold coin with a person's face, a silver coin with a fork and knife, a red coin with the word 'MEGACoin', a blue coin with a white 'Q' and a hat, a yellow coin with a white 'F', a silver coin with a white 'Z', a gold coin with a white 'Pi', a silver coin with a white 'L', a gold coin with a white 'D' and a dog, a silver coin with a white 'E', a gold coin with a white 'B', a silver coin with a white 'F', a gold coin with a white 'K', a silver coin with a white 'M', a gold coin with a white 'N', a silver coin with a white 'O', a gold coin with a white 'P', a silver coin with a white 'R', a gold coin with a white 'S', a silver coin with a white 'T', a gold coin with a white 'U', a silver coin with a white 'V', a gold coin with a white 'W', a silver coin with a white 'X', a gold coin with a white 'Y', and a silver coin with a white 'Z'. The coins are arranged in a circular pattern, creating a dense and colorful composition.

Blockchain

I

Initial

C

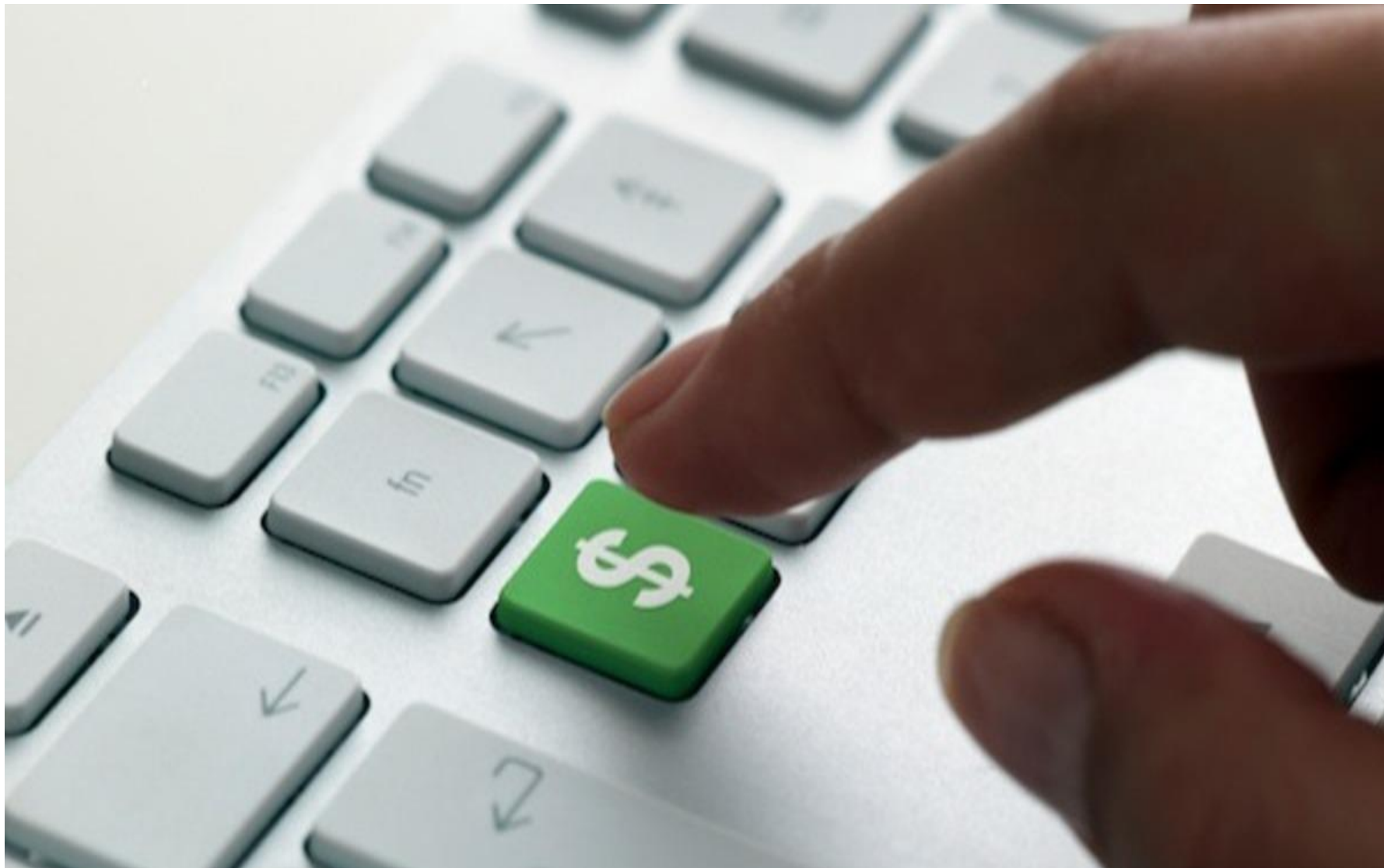
Coin



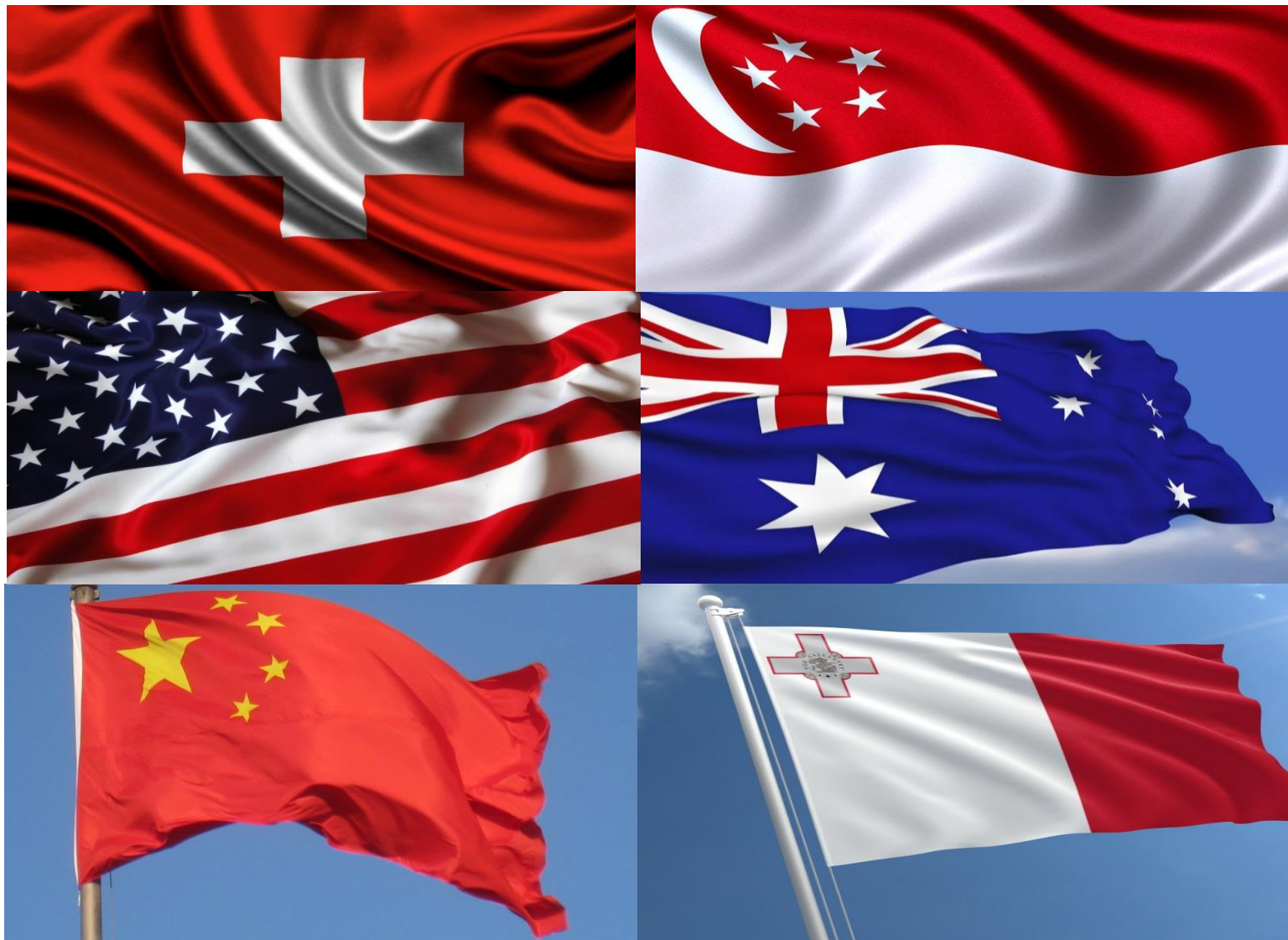
Offering

A Beginners Guide

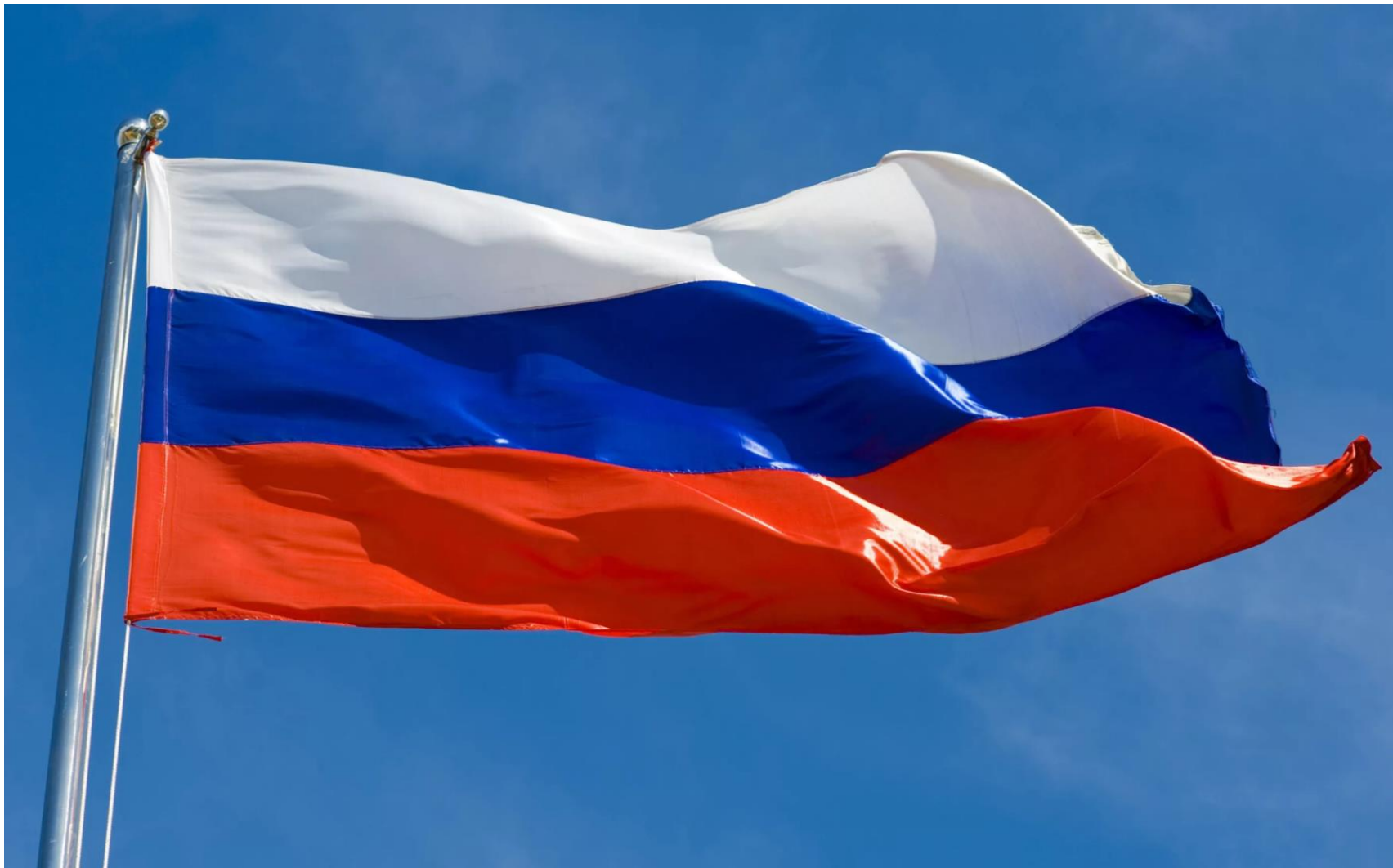
Как заработать?



Вопросы регулирования / В мире



Вопросы регулирования / В России / ЦБ Vs. Минфин



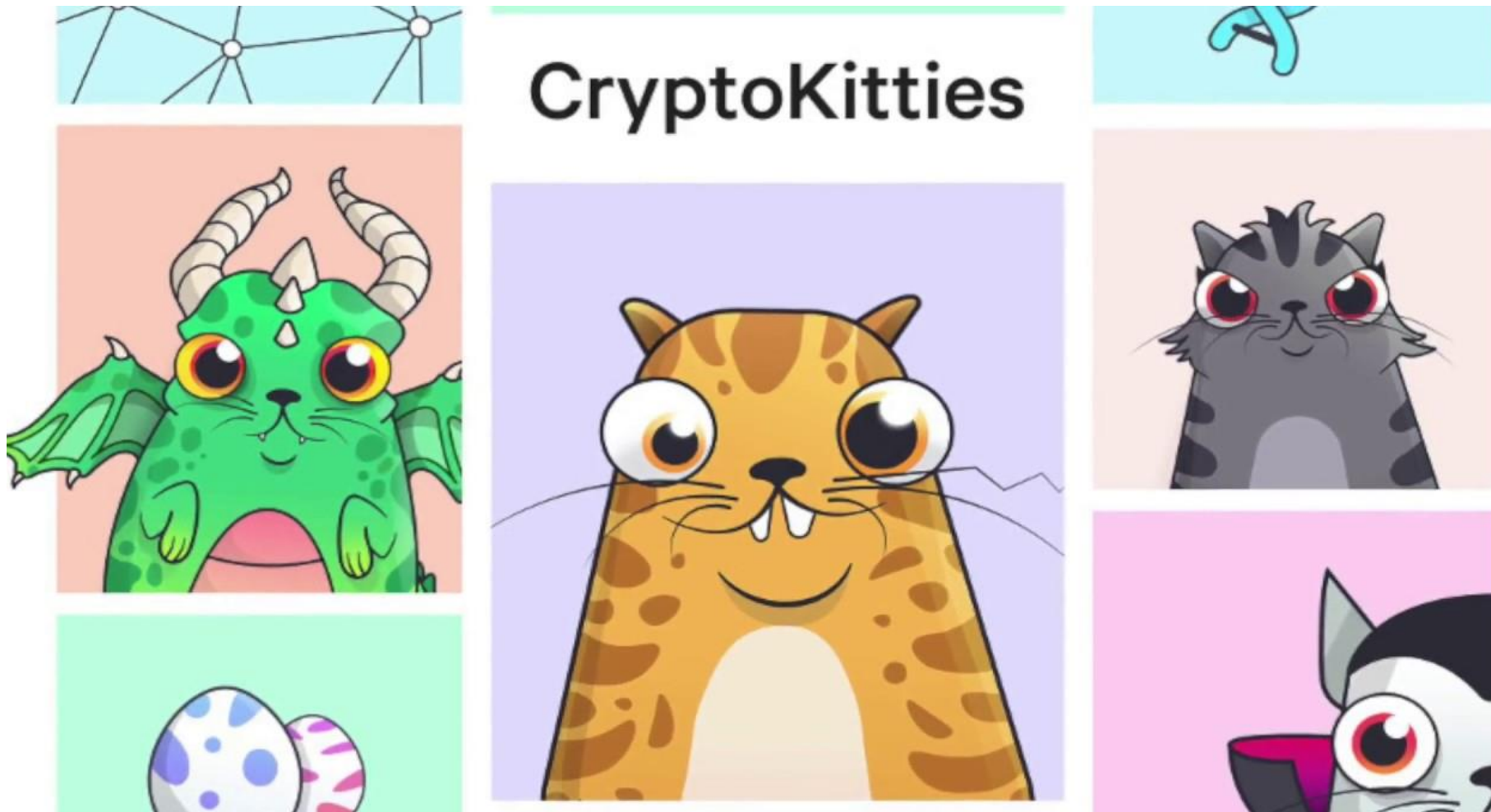
Риски



Цифровая экономика



Забавные факты



Контакты



Антон Поддубный

Советник, Корпоративная практика и M&A

T +7 812 325 84 44

M +7 921 960 83 36

anton.poddubny@dentons.com

Dentons – крупнейшая в мире юридическая фирма*, предоставляющая полный спектр юридических услуг. Dentons входит в число лидеров рейтинга ведущих юридических брендов мира, составленный Acritas, получила награду BTI Client Service 30 Award, а также – высокую оценку деловых и юридических изданий за инновации, включая создание Nextlaw Labs и Nextlaw Global Referral Network. Dentons предоставляет юридические услуги российским и иностранным компаниям, банкам и другим финансовым институтам, фондам прямых инвестиций, государственным предприятиям и некоммерческим организациям.

www.dentons.com

** 2017 The American Lawyer – Рейтинг 100 международных юридических фирм по количеству юристов (Global 100).*

© 2018 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. Please see dentons.com for Legal Notices.



Association
of European
Businesses

AEB North-Western Regional Committee

THANK YOU!

Address: Finlyandsky Prospekt 4a, 194044 St. Petersburg, Russian Federation

Tel.: +7 (812) 458 58 00, +7-911-012-6746

E-mail: spb@aebrus.ru

www.aebrus.ru