Банк России

ХИЩЕНИЯ С КАРТ И СЧЕТОВ

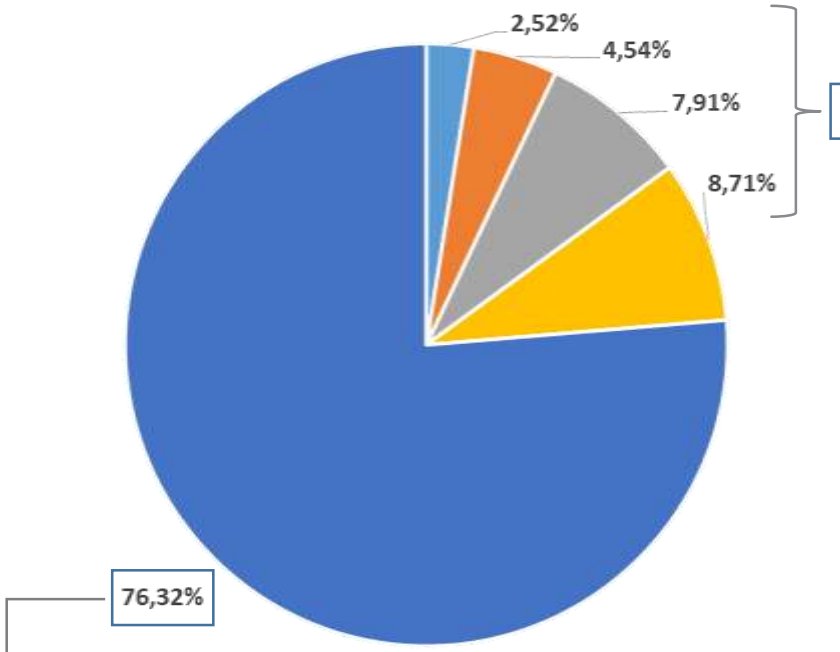
СЛУЧАИ С КОТОРЫМИ МОЖЕТ СТОЛКНУТЬСЯ КАЖДЫЙ

2021 г.

Банк России

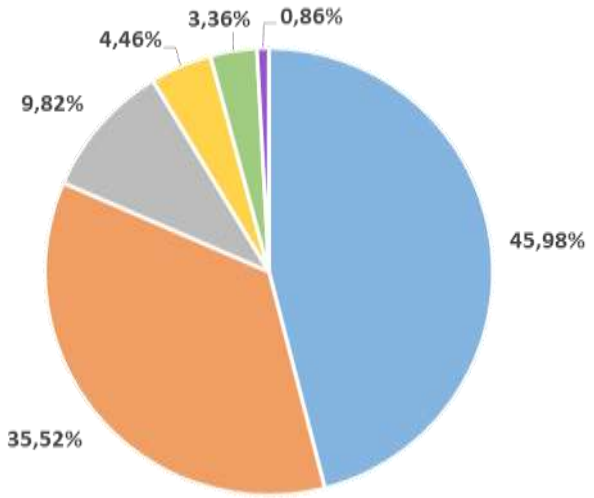
Основные каналы и способы осуществления операций без согласия
(результаты опроса кредитными организациями своих клиентов за I и II кв. 2021 года)

Основные каналы атаки, используемые злоумышленником

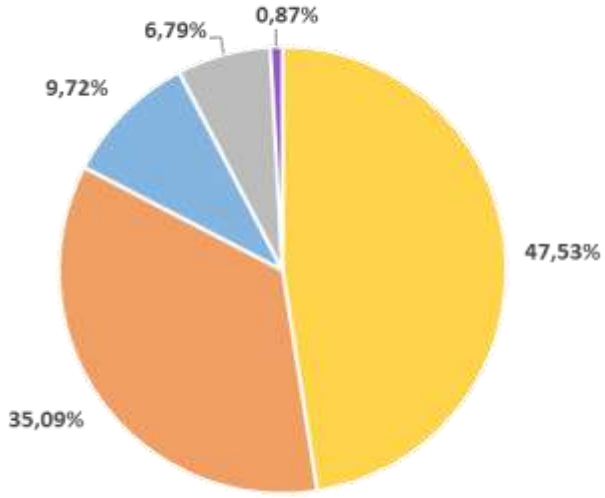


Действия пострадавшего

При поступлении звонка на мобильный телефон



При осуществлении атаки в иных каналах



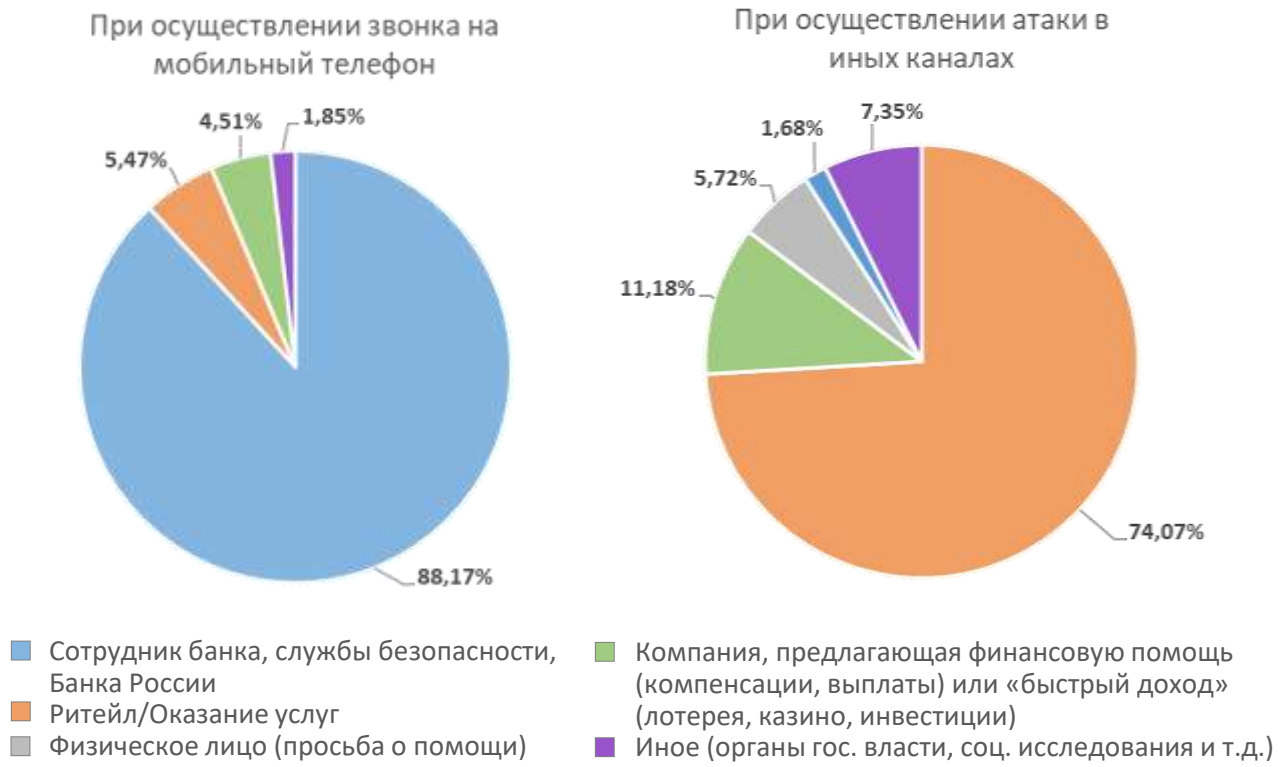
Социальная инженерия остается основной причиной совершения операций без согласия клиента.

Основным каналом, используемым злоумышленниками по-прежнему является ***звонок на мобильный телефон*** с целью получения данных, необходимых для совершения операции.

Банк России

Основные тематики звонков и сообщений злоумышленников
(результаты опроса кредитными организациями своих клиентов за I и II кв. 2021 года)

Способ маскировки злоумышленника



При осуществлении звонка на мобильный злоумышленники чаще всего представляются ***сотрудниками банка***. Успешной атаке способствует наличие у злоумышленника персональных данных жертвы.

В иных каналах злоумышленники предпочитают маскироваться под ***продавцов и покупателей*** товара.

Банк России

Объем операций без согласия клиента в общем объеме операций (по данным форм отчетности, направленных в Банк России)*

2019 год – 6,43 млрд рублей

2020 год – 9,79 млрд рублей

Половина 2021 года – 5,85 млрд рублей

При сохранении темпов роста объемов операций без согласия клиентов к концу 2021 года можно ожидать ущерб в 12 млрд рублей.

*Формы отчетности 0403203, 0409250, 0409251. Период сбора: 1 кв. 2019 – 2 кв. 2021. Дата актуализации данных: 22.07.2021.

Основные принципы защиты

1. Не сообщайте персональные данные, данные карт, коды подтверждения людям, которые звонят вам
2. Не совершайте ни каких действий под руководством неизвестных лиц
3. Вы не знаете кто вам звонит – всегда считайте, что вам звонит злоумышленник
4. В любой непонятной ситуации завершайте разговор и самостоятельно обращайтесь в банк

С чем может столкнуться каждый ВХОДЯЩИЙ ЗВОНОК

1. Сотрудник банка или робот

2. Работник правоохранительных органов

3. Юридическая помощь

4. Финансовый советник

С чем может столкнуться каждый ВХОДЯЩЕЕ СООБЩЕНИЕ

1. О блокировке ваших карт и счетов

2. О поступлении, которого вы не ждали, с последующим звонком или сообщением с просьбой вернуть деньги

3. О попытке кражи ваших денег

4. Код подтверждения операции с последующим звонком

С чем может столкнуться каждый
ПИСЬМО НА ЭЛЕКТРОННУЮ ПОЧТУ

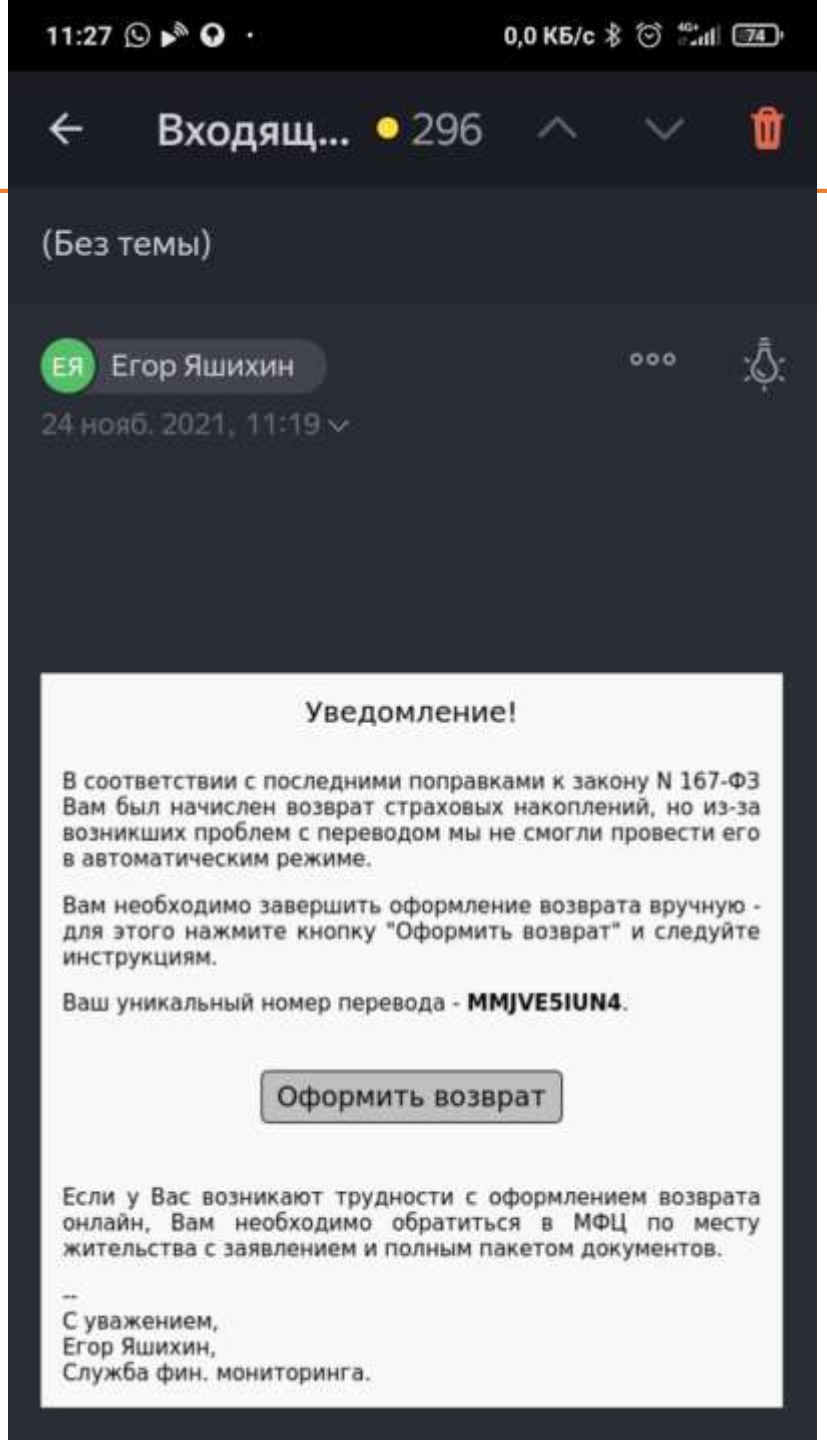
1. В письме может быть вирус (блокировщик, шифровальщик и т.д.)

2. В письме может быть ссылка на поддельный ресурс

3. Ссылка на фишинговый сайт

4. Информация юридической помощи (льготы, возмещения)

Конкретный пример мошенничества



Выводы

1. Не сообщайте людям, которые Вам звонят, свои персональные данные, данные карт, коды подтверждения
2. Не совершайте никаких действий под руководством неизвестных лиц
3. Если Вы не знаете того, кто Вам звонит, всегда считайте, что это злоумышленник
4. В любой непонятной ситуации завершайте разговор и самостоятельно обращайтесь в банк

Если они оказались хитрее

1. Заблокируйте карту, с которой произошло хищение
2. Напишите в банк заявление о несогласии с операцией и заявление на возврат утраченных средств
3. Напишите заявление в полицию
4. Проконсультируйтесь с юристом

Помните, что возмещение похищенных с электронных средств платежа регламентируется статьей 9 Федерального закона от 27.06.2011 №161-ФЗ «О национальной платежной системе». Возмещение возможно ТОЛЬКО если вы не нарушали требований безопасности при использовании электронных средств платежа и незамедлительном (обращении с заявлением о не согласии с операцией в ваш банк.

Банк России

Хотите узнать больше о финансах?

Образовательный сайт Банка России

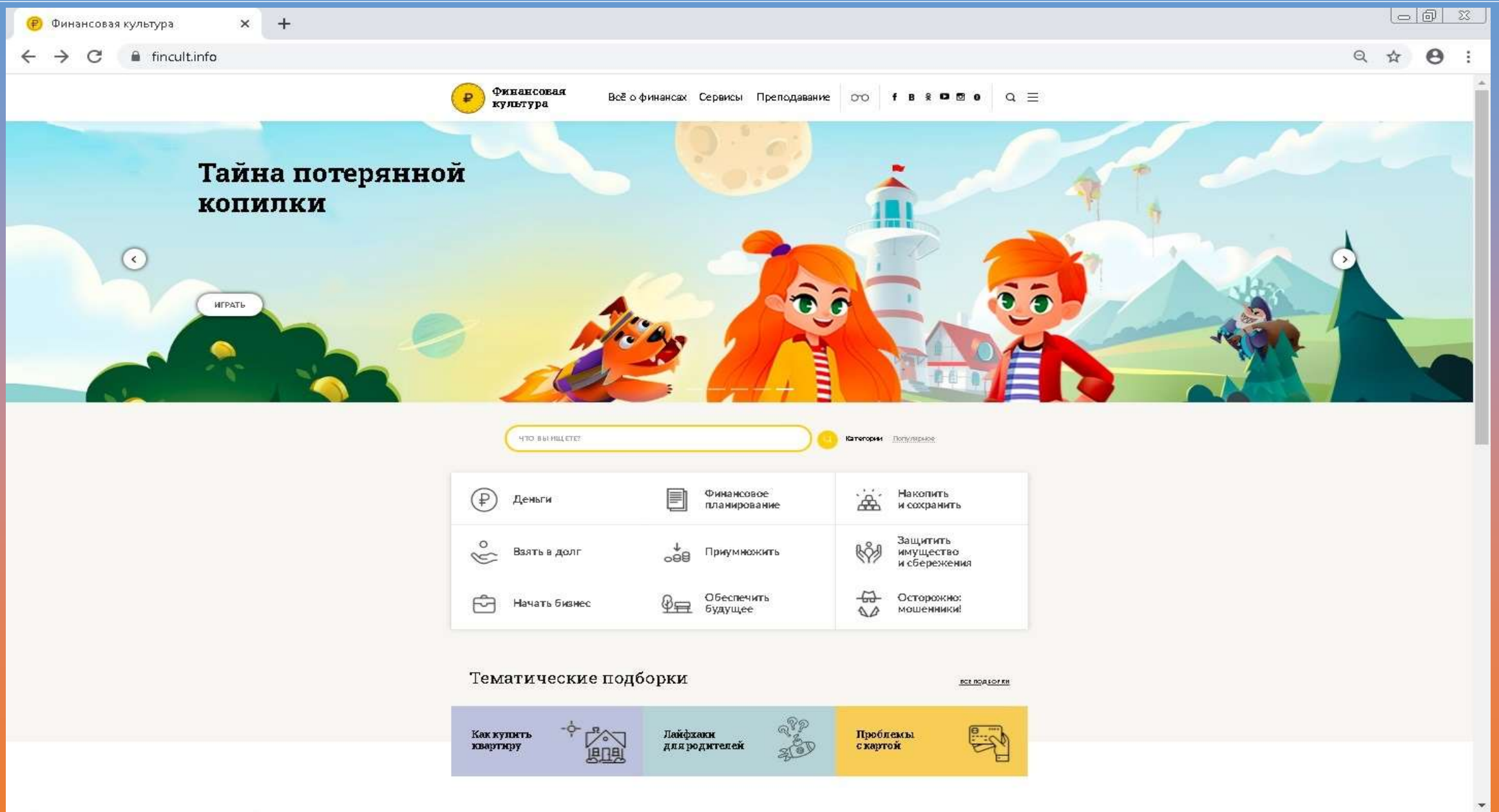
Fincult.info

Сайт онлайн-уроков Банка России

Dni-fg.ru

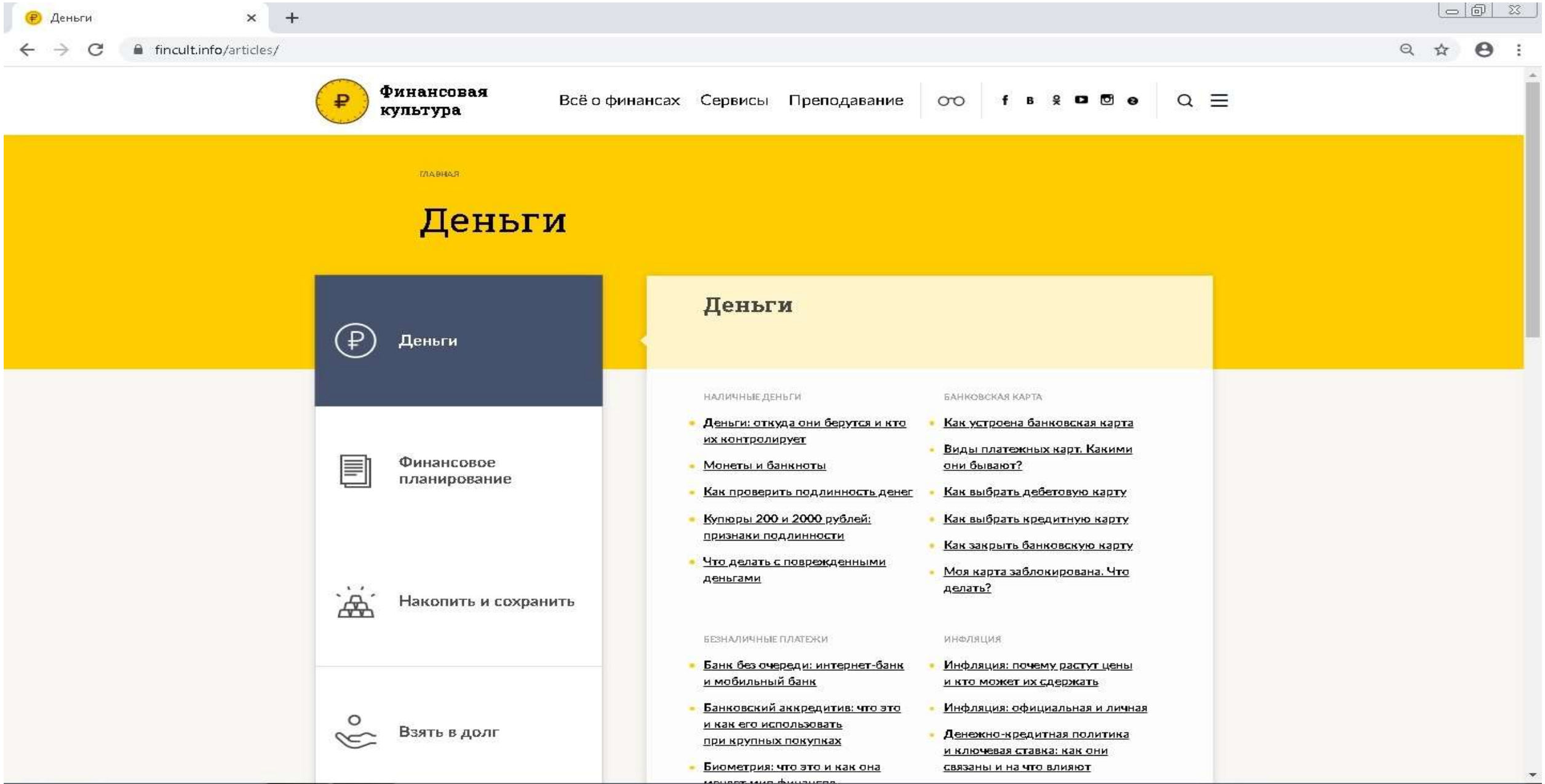
Банк России

FINCULT.INFO



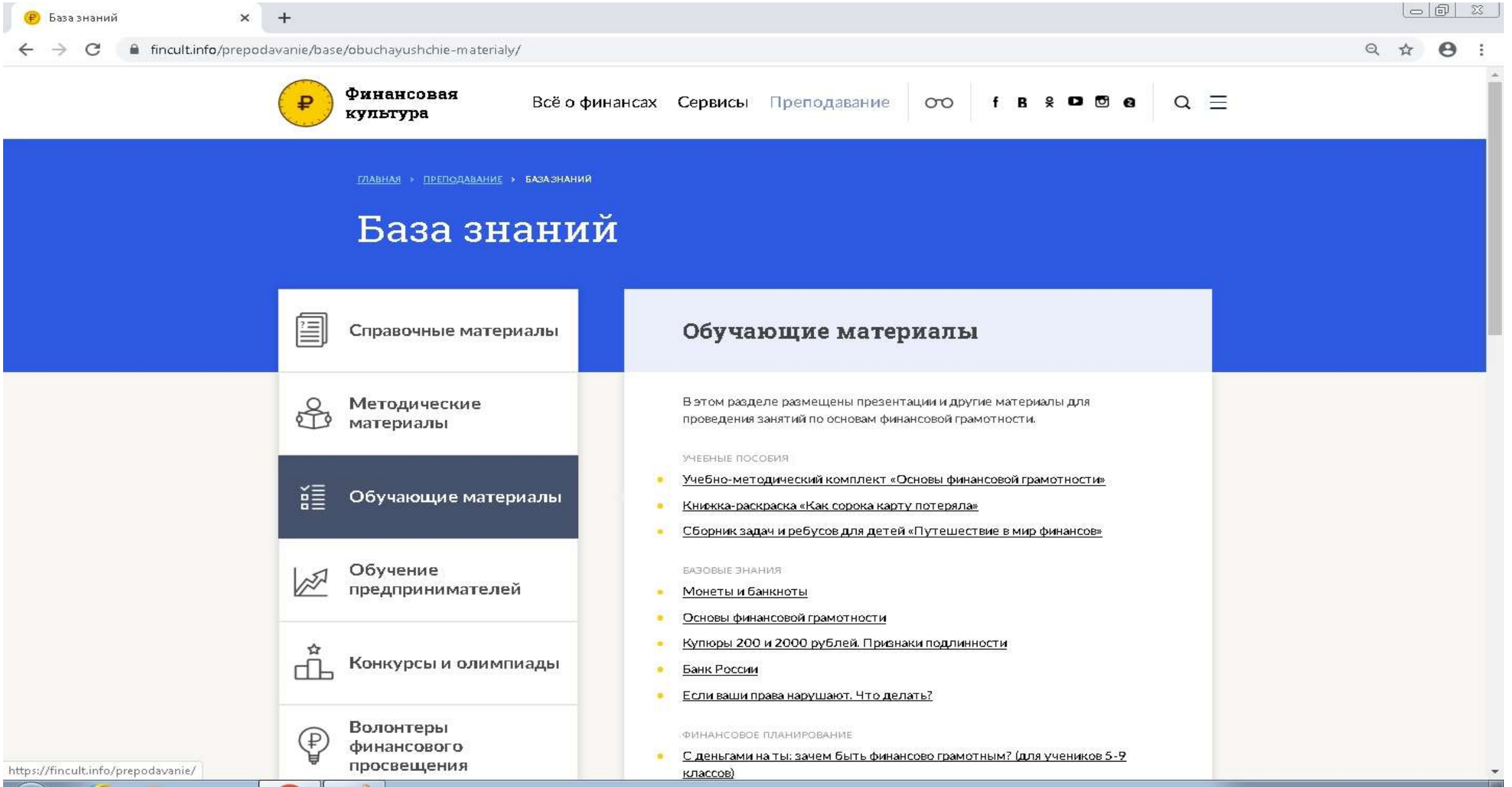
Банк России

FINCULT.INFO



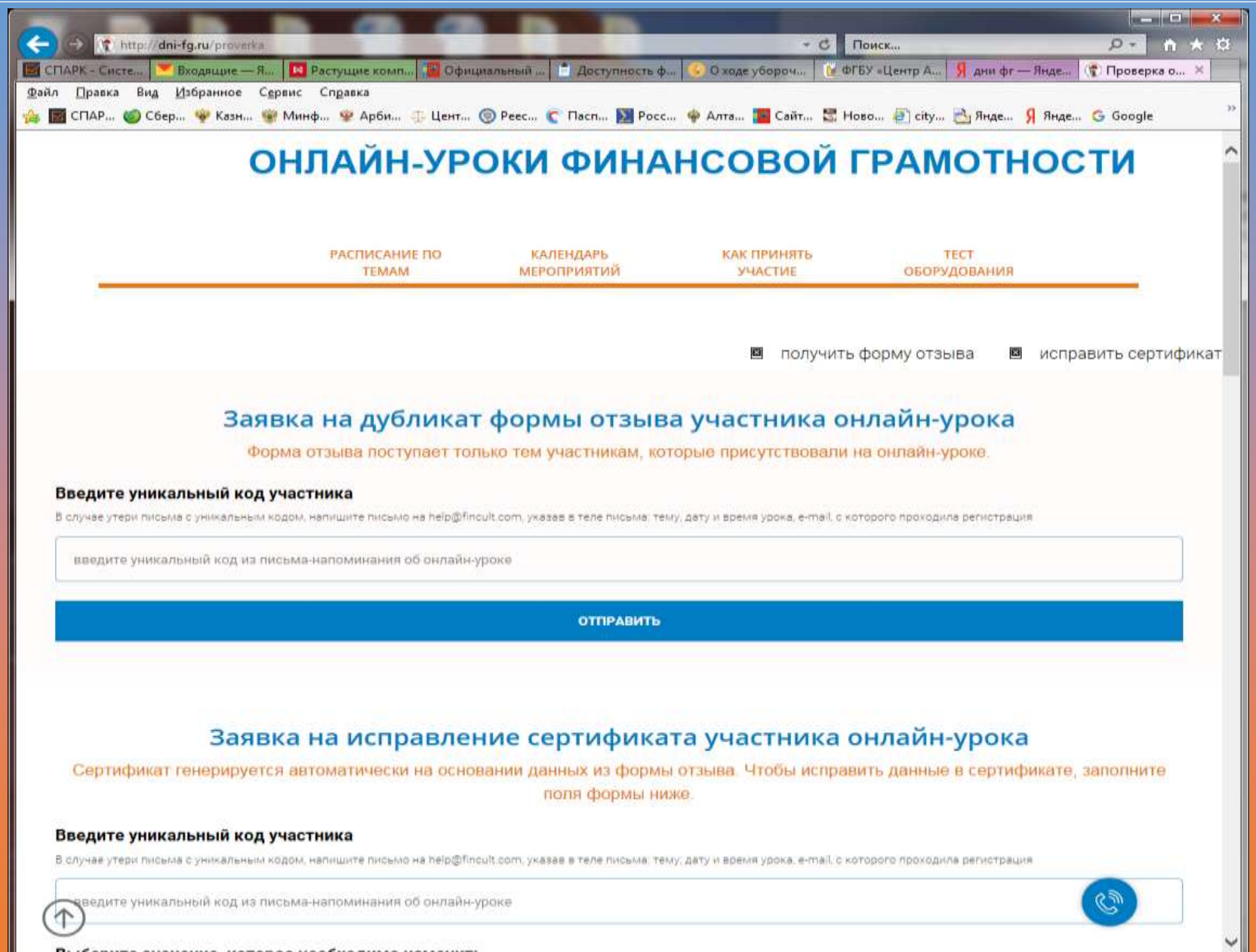
Банк России

FINCULT.INFO



Банк России

ОНЛАЙН-УРОКИ БАНКА РОССИИ dni-fg.ru



Спасибо за внимание!

МЕТЕЛЕВ МИХАИЛ ВЛАДИМИРОВИЧ
8-913-252-30-65
MetelevMV@cbr.ru

ГАЛЕНКО ВЛАДИМИР АЛЕКСАНДРОВИЧ
8 (3852) 388-630
GalenkoVA@cbr.ru