



# Деятельность Банка России по повышению безопасности платежных услуг с применением технологий дистанционного банкинга

Р.А. Прохоров

заместитель директора  
Департамента национальной  
платежной системы  
Банка России



---

Декабрь 2013 г.  
г. Москва



# **Федеральный закон «О национальной платежной системе»**

Банку России предоставлены полномочия по:

- регулированию платежных систем
- осуществлению надзора и наблюдения в национальной платежной системе
- установлению требований по обеспечению защиты информации при осуществлении переводов денежных средств и контролю за их соблюдением



# Стратегия развития НПС

Стратегия развития НПС одобрена Советом директоров Банка России 15 марта 2013 года

План мероприятий Банка России по реализации Стратегии развития НПС утвержден Председателем Банка России 2 августа 2013 года

Стратегия развития НПС определяет цель, факторы, принципы и направления развития НПС

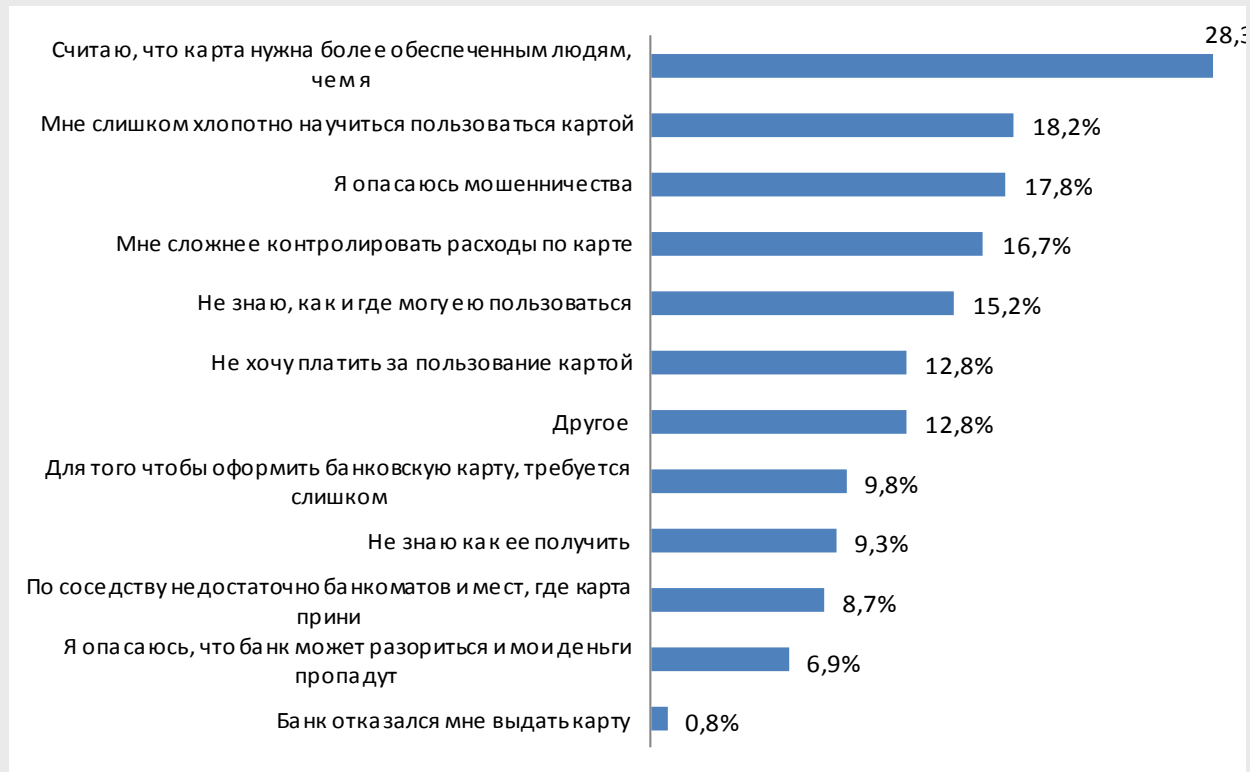
## **Целью развития НПС является:**

обеспечение эффективного и надежного функционирования субъектов НПС для удовлетворения текущих и перспективных потребностей национальной экономики в платежных услугах, в том числе для реализации денежно-кредитной политики, обеспечения финансовой стабильности, повышения качества, доступности и **безопасности платежных услуг**



# Поведение потребителей (обследование)

Диаграмма. Причины отсутствия банковской карты.



Количество респондентов: 1072.



# Основные нормативные акты Банка России

382-П О требованиях по защите информации при переводах денежных средств

2831-У Об отчетности по защите информации при переводах денежных средств



## Рекомендации Банка России

Письмо от 01.03.2013 №34-Т «О рекомендациях по повышению уровня безопасного использования банкоматов и платежных терминалов»

включает основные рекомендации, способствующие повышению уровня безопасного использования банкоматов и платежных терминалов, в том числе проведение классификации мест установок, использование видеонаблюдения

Письмо от 5.08.2013 №146-Т «О рекомендациях по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети «Интернет»

включает основные рекомендации, способствующие повышению уровня безопасности при предоставлении розничных платежных услуг с использованием сети «Интернет», в том числе проведение и использование результатов анализа рисков, осуществление мониторинга операций, использование лимитов и временных ограничений



## Основные направления деятельности (1)

Участие и инициация обсуждений проблемных вопросов на различных площадках – тематических конференциях, форумах и т.п.

Создание Консультативного совета по вопросам развития национальной платежной системы при Председателе Банка России

Повышение финансовой грамотности населения и осведомленности об угрозах нарушения безопасности розничных платежных услуг

Содействие внедрению лучших практик обеспечения защиты информации при осуществлении переводов денежных средств посредством участия в разработке соответствующих стандартов и рекомендаций по их внедрению

Работа Технического комитета № 122 «Стандарты финансовых операций» и его подкомитетов «Безопасность банковских (финансовых) операций», «Процедуры и технологии расчетов с использованием банковских карт и иных инструментов розничных платежей», «Мобильные платежи»

Формирование предложений по изменению законодательства (возврат средств по несанкционированным операциям, усиление ответственности, формирование и использование базы инцидентов)



## Основные направления деятельности (2)

Анализ деятельности поднадзорных организаций и кредитных организаций по данным отчетности и иных источников информации

Проведение инспекционных проверок поднадзорных организаций, кредитных организаций по вопросам обеспечения защиты информации при переводах денежных средств

Контроль готовности кредитных организаций к выполнению требований статьи 9 Закона о НПС

Публикация аналитических обзоров об инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств

Обследование уровня готовности кредитных организаций к выпуску и обслуживанию платежных карт с микропроцессором стандарта EMV

Опубликован обзор международных и российских подходов к противодействию несанкционированным операциям в сфере розничных платежных услуг





# Совершенствование регулирования (1)

Изменения в Положение Банка России № 382-П  
(вступают в силу по истечении 180 дней с 10 июля 2013 года)

Регистрация информации о действиях клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения:

- дата (день, месяц, год) и время (часы, минуты, секунды) осуществления действия клиента;
- идентификатор клиента
- код, соответствующий выполняемому действию;
- идентификационная информация - IP-адрес, MAC-адрес, номер SIM-карты, номер телефона и др.

Оператор по переводу денежных средств определяет во внутренних документах порядок хранения информации

Оператор по переводу денежных средств обеспечивает хранение информации не менее пяти лет, начиная с даты осуществления клиентом действия, выполняемого с использованием автоматизированной системы, программного обеспечения



## Совершенствование регулирования (2)

Изменения в Положение Банка России № 382-П  
(вступили в силу 10 июля 2013 года)

Организация, ставшая оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры, должна провести первую оценку соответствия\* в течение **шести месяцев** после получения соответствующего статуса

Организация, являющаяся на день вступления в силу настоящего Указания оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры, должна провести оценку соответствия\* в течение **шести месяцев** со дня вступления в силу Указания Банка России № 3007-У от 5 июня 2013 года (**вступило в силу 10 июля 2013 года**)

\* Оценка соответствия проводится самостоятельно или с привлечением сторонних организаций

Порядок проведения оценки соответствия и документирования ее результатов определен в приложении 1 к Положению № 382-П

Перечень проверяемых требований определен в приложении 2 к Положению № 382-П



## Совершенствование регулирования (3)

Планируемые изменения в Положении Банка России № 382-П:

- установление требований к обеспечению защиты информации при осуществлении переводов денежных средств с применением технологий Интернет-банкинга и мобильного банкинга
- установление требований к обеспечению защиты информации при осуществлении переводов денежных средств с применением банкоматов и платежных терминалов
- установление требований к обеспечению защиты информации при осуществлении переводов денежных средств с применением платежных карт, оснащенных магнитной полосой и (или) микропроцессором, выданных (эмитированных) кредитными организациями на территории Российской Федерации



## Совершенствование регулирования (4)

Требования к обеспечению защиты информации при осуществлении переводов денежных средств с применением технологий Интернет-банкинга и мобильного банкинга

Определены понятия «Интернет-банкинг» и «мобильный банкинг».

Устанавливаются требования к :

- предоставлению клиенту возможности установления лимитов и наложения иных ограничений на функциональность систем Интернет-банкинга
- применению технологий подтверждения переводов денежных средств (одноразовых и многократных паролей и генерирующих их устройств), конкретизация требований к уведомлениям, направляемым клиентам до подтверждения перевода денежных средств
- разработке и распространению (в том числе, через репозитории мобильных приложений и иные общедоступные ресурсы) систем Интернет- и мобильного банкинга
- предоставлению клиенту возможности блокировки платежных карт через системы Интернет-банкинга
- предоставлению клиенту возможности блокировки систем Интернет-банкинга
- взаимодействию операторов по переводу денежных средств и операторов подвижной радиотелефонной связи с целью предотвращения дистанционного банковского обслуживания с использованием абонентских номеров, обслуживание которых прекращено



## Совершенствование регулирования (5)

Требования к обеспечению защиты информации при осуществлении переводов денежных средств с применением банкоматов и платежных терминалов

Устанавливаются детализированные требования к :

- организации и проведению настройки (в том числе удаленной) ТУ ДБО\*
- внесению изменений в программно-аппаратное обеспечение ТУ ДБО
- техническому обслуживанию и модернизации ТУ ДБО
- контролю загрузки и (или) изъятия наличных денежных средств
- организации сетей, объединяющих банкоматы
- видеонаблюдению за ТУ ДБО
- взаимодействию с клиентом, в том числе требований к приему обращений клиентов о возможных нарушениях защиты информации, требований о размещении информации на дисплее и корпусе ТУ ДБО
- периодическому контролю состояния ТУ ДБО

\* ТУ ДБО - терминальные устройства дистанционного банковского обслуживания



## Совершенствование регулирования (6)

Требование применения платежных карт, оснащенных микропроцессором, выданных (эмитированных) кредитными организациями на территории Российской Федерации

Обязательное оснащение вновь выпускаемых карт микропроцессором, что обусловит плавный переход кредитных организаций на выпуск микропроцессорных карт.

Карты могут комплектоваться магнитной полосой и иными средствами наряду с микропроцессором, наличие которого обязательно.

Данное требование распространяется только на платежные и расчетные карты (предоплаченные карты смогут выпускаться без чипа).

Вторая часть изменений предусматривает запрет на осуществление эквайринга карт с использованием магнитной полосы (исключительно в отношении переводов денежных средств, операции по внесению и снятию денег будут доступны держателям карт с магнитной полосой) и условия снятия данного запрета (например, при выезде за границу).



## Совершенствование регулирования (7)

### Изменения в Указание Банка России № 2831-У

(вступают в силу 28 января 2014 года)

- Уточнение критериев включения инцидентов в отчетность
- Уточнение параметров, описывающих инциденты
  - Даты – выявления, возникновения инцидента, завершения разбирательства по нему
  - Условия возникновения инцидента
  - Описание инцидента
  - Причины инцидента
  - Регион выявления инцидента
  - Отношения к платежной системе
  - Последствия инцидента
- Введение оценок ущерба
- Дополнение новым разделом: «Сведения об инцидентах предыдущих отчетных периодов»
- Уточнение сроков представления отчетности



**До новых встреч!**