



Безопасность финансовых услуг –
ключевое направление для успешного
развития банковского бизнеса

Исполнительный директор АРБ
Шипилов В.В.



Статья 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»

С 01 января этого года вступило в силу требование статьи 9 Закона № 161-ФЗ «О национальной платежной системе» об обязательном информировании клиентов о совершении каждой операции, а также об ответственности кредитных организаций за их неуведомление.

Типовые уведомления:

- SMS-сообщения,
- электронная почта,
- личные кабинеты и др.

Предпочтения - SMS-сообщения, т.к. они являются

- **важным способом снижения рисков** банков и их клиентов при осуществлении безналичных расчетов;
- **самым удобным и доступными для клиента каналом доставки информации** о движении средств по счетам.



VI Уральский форум “Информационная безопасность банков”


ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Банк России)

Московское главное
территориальное управление

115035, Москва, ул. Балчуг, 2

от 18.12.2013 № [redacted]

На № _____

Ответ на обращение

Уважаемый Павел Михайлович!

В ответ на Ваше обращение в Интернет-приемную Банка России от 18.11.2013 касательно изменения тарифов операторов сотовой связи в связи с выполнением кредитными организациями требований статьи 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе», Московское ГТУ Банка России с учетом позиции Департамента национальной платежной системы Банка России сообщает следующее.

Банк России не располагает подтверждающей информацией о намерении операторов сотовой связи повысить тарифы по отправке SMS – сообщений.

Кроме того, вопрос о действиях операторов сотовой связи, нарушающих антимонопольное законодательство, в частности статью 11.1 Федерального закона от 26 июля 2006 года № 135-ФЗ «О защите конкуренции», относится к компетенции Федеральной антимонопольной службы России.

Заместитель начальника

С.В. Абляев

Однако, в конце 2013 года крупные OCC повысили тарифы, объяснив это якобы необходимостью борьбы с «коммерческими SMS-рассылками».

На самом деле коммерческими SMS были признаны все SMS вне зависимости от их содержания.

Таким образом, в категорию «коммерческих SMS» попадают сообщения банков

- о транзакциях,
- коды подтверждений
- и другие,

которые КО отправляют по соглашению с их получателями, и на которых **не зарабатывают денег**, а лишь предоставляют сервисы, минимизирующие финансовые риски граждан и организаций.

Ряд банков пытались самостоятельно обращаться как в Банк России (см. письмо в МГТУ), так и другие организации, в том числе и АРБ.

Ассоциация российских банков в декабре 2013 г. на специальной рабочей группе обсудила этот вопрос с банковским сообществом, пригласив на эту встречу представителей ОСС. По итогам встречи банки обратились к АРБ с просьбой написать письмо в ФАС.

Для сбора объективной информации [на портале АРБ](#) было организовано обсуждение сложившейся ситуации.

Главная цель этого обсуждения – выяснить насколько «объективна» попытка ОСС использовать ситуацию и повысить тарифы в связи с вступлением статьи 9 и нарушается ли антимонопольное законодательство, т.к. для направления письма в ФАС – нужны объективные аргументы.

Подключайтесь к этому процессу!

Аргументируйте!



О «Государственном центре реагирования на компьютерные инциденты»

1. Банкам приходится работать в условиях воздействия постоянно обновляющихся методов и технологий противоправной деятельности, в том числе основанных на использовании средств коммуникации и информационных технологий.

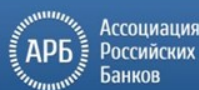
Примером может быть ДБО, особенностью которого является то, что нападение осуществляется не на один банк, а через цепочку кредитных организаций. Поэтому банку-плательщику практически невозможно противостоять этим действиям в одиночку.

2. Однако при взаимодействии банков как между собой, так и с правоохранительными органами возникают правовые проблемы, т.к. противодействие киберпреступности силами МВД России и ФСБ России строго регламентировано законодательством Российской Федерации, которое в настоящее время не вполне учитывает особенности противоправных действий с использованием современных информационных технологий.

3. Опыт зарубежных стран показывает, что эффективное противодействие киберугрозам возможно лишь с помощью **государственных центров реагирования на компьютерные инциденты** (Computer Emergency Response Team – CERT).



VI Уральский форум “Информационная безопасность банков”



Центр реагирования на компьютерные инциденты Computer Emergency Response Team – CERT



Республика Башкортостан, ДЦ “Юбилейный”,
17-22 февраля 2014 г.

Организационное начало CERT:

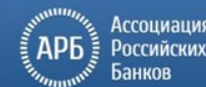
- *под патронажем государства;*
- *некоммерческая;*
- *государственное финансирование;*

Основные функций CERT:

- **мониторинг инцидентов** информационной безопасности;
- **сбор и анализ информации** о выявленных уязвимостях информационно-технологических средствах, используемых в банках;
- **анализ и прогнозирование рисков** и проблемных ситуаций, связанных с информационно-телекоммуникационными технологиями, применяемыми в кредитных организациях банковской системы Российской Федерации;
- **организационная и методическая помощь** в локализации и расследовании инцидентов, включая взаимодействие с правоохранительными органами и пр.



VI Уральский форум “Информационная безопасность банков”



Учитывая актуальность этой темы, **20 февраля** планируется в рамках Конференции провести пресс-коктейль **«Нужно ли создание Банковского центра реагирования на инциденты?»**, на котором хотели бы услышать мнение всех заинтересованных сторон, в том числе и **ЦБ РФ о целесообразности создания Государственного центра реагирования на компьютерные инциденты**, а также о **возможности координации Банком России** работы как по его организации, так и по совершенствованию законодательства в области противодействия противоправной деятельности с использованием информационных технологий.



V Уральский форум “Информационная безопасность банков”



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

2013

Республика Башкортостан, ДЦ “Юбилейный”,
11-16 февраля 2013 г.



«Обзор международных и российских подходов к противодействию несанкционированным операциям в сфере розничных платежных услуг»

II. Международный подход к противодействию совершению несанкционированных операций

Общеввропейские подходы

К декабрю 2008 года на территории европейских стран в течение

неск **Англия**

опер В Англии к организациям, занимающимся противодействием

Европ совер

Соединенные Штаты Америки

плате В США вопросы безопасного дистанционного банковского

Канада

Одним из направлений деятельности полиции Канады является проведение

мер **Австралия**

опер Основанная Координационным Комитетом Реформы Клиринговой Системы в
публ 1992 году саморегулирующаяся «Австралийская Ассоциация Платежного
Клиринга» («Australian Payments Clearing Association», далее -ААПК) ...

СТИ



VI Уральский форум “Информационная безопасность банков”

«Обзор международных и российских подходов к противодействию несанкционированным операциям в сфере розничных платежных услуг»

III. Российский подход к противодействию совершению несанкционированных операций

В Российской Федерации существуют различные инициативы по

- п
и
с
с
1. По инициативе **Банка России** была начата деятельность по разработке национального стандарта финансовых операций на основе **стандарта ISO 20022**, который является принятой в международной практике методологией описания процедур осуществления финансовых операций и форматов финансовых сообщений. **В декабре 2010 года** в соответствии с приказом Федерального агентства по техническому регулированию и метрологии на добровольной основе создан заинтересованными организациями **Технический комитет по стандартизации № 122 «Стандарты финансовых операций»** (далее – ТК № 122) в
 - цел
меж 2. В рамках «Ассоциации Российских членов Европей» (АРЧЕ), «Ассоциации российских банков» (АРБ) и «Сообщества ABISS» в 2009 году реализован проект по созданию межбанковского информационного ресурса, обеспечивающего закрытый канал обмена данными по инцидентам с платежными картами и информационной безопасностью.

Данная система позволяет банкам:

- быстро и с большой точностью выявлять точки компрометации ПК;
- своевременно блокировать компрометированные карты;
- получать дополнительную, как правило, достоверную информацию при проведении претензионной работы по заявлениям клиентов;
- выявлять новые мошеннические схемы и вырабатывать меры противодействия;
- обмениваться практическим опытом в области борьбы с мошенничеством;
- вести профессиональный диалог с правоохранительными органами и информировать банковское сообщество о соответствующих судебных решениях и др.

В настоящее время сертифицированными пользователями Форума являются около **600** представителей из более чем **200** банков России, Армении, Украины, Белоруссии, Молдавии и Казахстана. В среднем, каждый день в системе появляется около **50** новых сообщений.



Практика эксплуатации системы в течение 5 лет показала, что она

- *реально снижает риски и финансовые потери как банков, так и клиентов;*
- *позволяет повысить эффективность ведения претензионной работы, что очень важно с учётом статьи 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платёжной системе»;*
- *заслужила уважительное отношение со стороны правоохранительных органов.*



Пример

*выявления фактов установки фальшивых банкоматов
в Москве, аэропорту «Внуково» и г. Сочи.*

Лето 2013 года.

Благодаря анализу информации, обсуждавшийся на Форуме, одним из участников было высказано предположение о возможной установке в ТЦ «Охотный ряд» (Москва) фальшивого банкомата.

В ходе осмотра ТЦ по ряду признаков был выявлен банкомат, который действительно оказался фальшивым. При этом, отличить его от настоящего было бы практически невозможно, если бы не было поставлено такой задачи.

Аналогичным образом были выявлены такие же банкоматы в аэропорту «Внуково» и в ТЦ в г. Сочи.

После привлечения сотрудников БСТМ МВД РФ, были возбуждены уголовные дела.

Следствие продолжается!



Присоединяйтесь!

Пользуйтесь!



VI Уральский форум “Информационная безопасность банков”

АРБ
Ассоциация
Российских
Банков

**Благодарю за
внимание!**

Республика Башкортостан, ДЦ “Юбилейный”,
17-22 февраля 2014 г.