Доклад:

Нормативное регулирование ДБО в России

Царев Евгений

конференция
РусКрипто'2013

http://www.ruscrypto.ru/conference/

Общая структура нормативных документов

161 – ФЗ
О национальной платежной системе

115-ФЗ
О противодействии легализации …

152 – ФЗ
О персональных данных

…

382 - П

2831-У

Письма Банка России

СТО БР ИББС

Методические рекомендации НП «НПС», АРБ

Письма Банка России

Письмо Банка России от 30.08.2006 **№ 115-Т** «Об исполнении 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" в части идентификации клиентов, обслуживаемых с использованием технологий ДБО (включая интернет-банкинг)»

Письмо Банка России от 05.04.2007 **№ 44-Т** «О проверке осуществления кредитными организациями идентификации клиентов, обслуживаемых с использованием технологий ДБО (включая интернет-банкинг)»

Письмо Банка России от 27.04.2007 **№ 60-Т** «Об особенностях обслуживания кредитными организациями клиентов с использованием технологии дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)»

Письмо Банка России от 07.12.2007 **№ 197-Т** «О рисках при ДБО»

Письмо Банка России от 31.03.2008 **№ 36-Т** «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем Интернет-банкинга»

Письмо Банка России от 30.01.2009 **№ 11-Т** «О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга»

Письмо Банка России от 26.10.2010 **№ 141-Т** «О рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания»

Письмо Банка России от 30.08.2006 N 115-Т

Письмо Банка России от 30.08.2006 **№ 115-Т** «Об исполнении 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" в части идентификации клиентов, обслуживаемых с использованием технологий ДБО (включая интернет-банкинг)»

✓Требование об идентификации лиц, которым предоставляются полномочия по распоряжению банковским счетом (банковским вкладом) с использованием ДБО

Письмо Банка России от 05.04.2007 N 44-Т

Письмо Банка России от 05.04.2007 **№ 44-Т** «О проверке осуществления кредитными организациями идентификации клиентов, обслуживаемых с использованием технологий ДБО (включая интернет-банкинг)»

Письмо разработано в целях повышения эффективности проведения проверок соблюдения кредитными организациями № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»

✓Рекомендуется установить, осуществлено ли кредитной организацией в соответствии с Инструкцией Банка России N 28-И установление личности лица (лиц), уполномоченного распоряжаться денежными средствами, находящимися на счете

✓**Отнесены ли** в соответствии с Положением Банка России N 262-П операции клиентов, осуществляемые с использованием интернет-технологий, **к операциям повышенной степени (уровня) риска их совершения в целях легализации (отмывания) доходов,** полученных преступным путем, или финансирования терроризма

Письмо Банка России от 27.04.2007 № 60-Т

Письмо Банка России от 27.04.2007 **№ 60-Т** «Об особенностях обслуживания кредитными организациями клиентов с использованием технологии дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)»

✓Рекомендуется **включать в договоры право** кредитной организации **отказывать клиенту в приеме от него распоряжения** на проведение операции по банковскому счету (вкладу), подписанному аналогом собственноручной подписи

✓Кредитным организациям **рекомендуется после предварительного предупреждения отказывать клиентам в приеме от них распоряжений** на проведение операции по банковскому счету (вкладу), **подписанных аналогом собственноручной подписи,** в случае выявления **сомнительных операций клиентов**. При этом кредитным организациям рекомендуется принимать от таких клиентов только надлежащим образом оформленные расчетные документы на бумажном носителе

Письмо Банка России от 07.12.2007 № 197

Письмо Банка России от 07.12.2007 **№ 197-Т** «О рисках при ДБО»

✓Рекомендовать кредитным организациям **включать в договоры,** заключаемые **с провайдерами Интернета, обязательства** сторон по принятию мер, направленных на **оперативное восстановление функционирования ресурса** при возникновении нештатных ситуаций, а также ответственности за несвоевременное исполнение таких обязательств **(DDoS)**

✓Банк России обращает внимание кредитных организаций на **необходимость распространения предупреждающей информации для своих клиентов,** в том числе с использованием представительств в сети Интернет (web-сайтов), о возможных случаях неправомерного получения персональной информации пользователей систем ДБО

Письмо Банка России от 31.03.2008 N 36-Т

Письмо Банка России от 31.03.2008 **№ 36-Т** «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем Интернет-банкинга»

- ✓Терминология (провайдер, система интернет-банкинга, и т.д.)
- ✓Основы для проведения анализа рисков для интернет-банкинга
- ✓Принципы управления рисками интернет-банкинга
- ✓Рекомендации к внутренней документации банка, устанавливающие порядок управления рисками интернет-банкинга
- ✓Информационное обеспечение управления рисками интернет-банкинга

Письмо Банка России от 30.01.2009 N 11-Т

Письмо Банка России от 30.01.2009 **№ 11-Т** «О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга»

- ✓Указание на возросшие риски несанкционированного списания денежных средств

- ✓Содержит положения о необходимости принятия дополнительных мер безопасности и контроля, например:
  - ✓Дополнить перечень потребляемых услуг безопасности от провайдера новыми (фильтрация трафика по требованию кредитной организации, информирование о проведении DDOS-атаки, принятие мер по нейтрализации DDOS-атак)
  - ✓Информирование клиентов о новых угрозах
  - ✓И т.д.

Письмо Банка России от 26.10.2010 № 141-Т

Письмо Банка России от 26.10.2010 **№ 141-Т** «О рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания»

✓Новая терминология (Защищенность ДБО, информационный контур ДБО, защищенность операций и т.п.)

✓Подход к выбору провайдеров основывается на анализе рисков

✓Оценивается возможности получения от провайдеров информации, необходимой кредитной организации для эффективного управления рисками, сопутствующими ДБО

Общая структура нормативных документов

161 – ФЗ
О национальной платежной системе

115-ФЗ
О противодействии легализации …

152 – ФЗ
О персональных данных

…

382 - П

2831-У

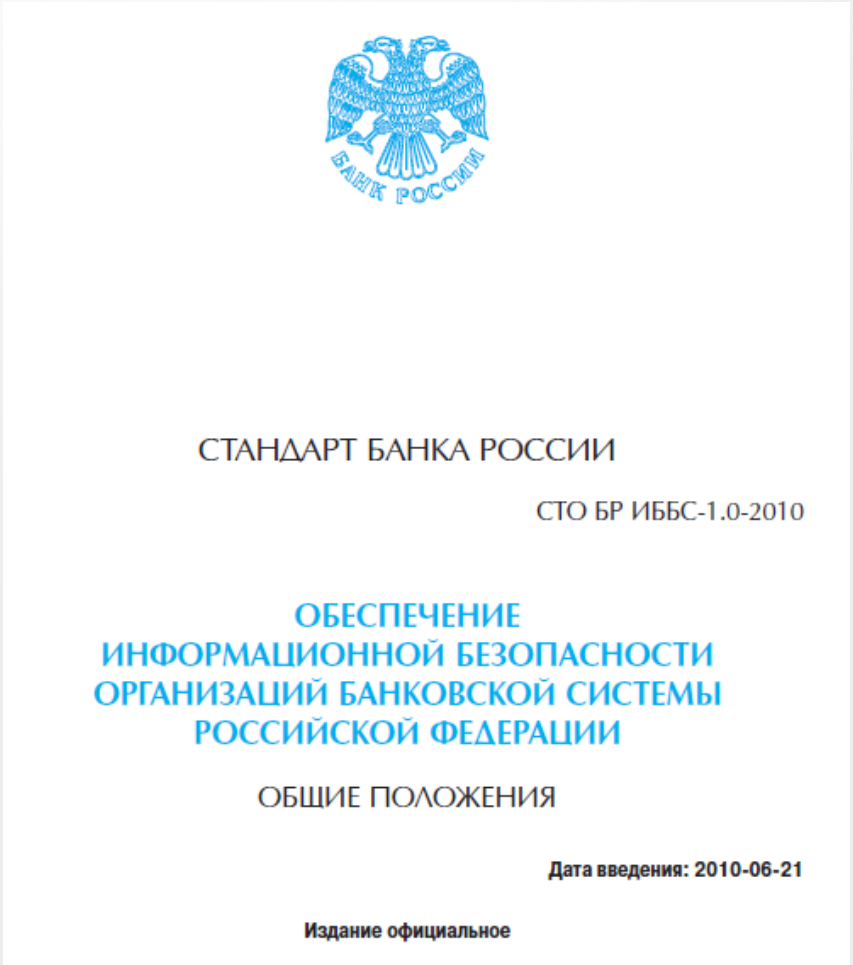
Письма Банка России

СТО БР ИББС

Методические рекомендации НП «НПС», АРБ

СТО БР ИББС

СТО БР ИББС-1.0-2010 «Общие положения»



СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.0-2010

ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения: 2010-06-21

Издание официальное

СТО БР ИББС-1.2-2010 «Методика оценки соответствия»

СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.2-2010

ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ
БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
ТРЕБОВАНИЯМ СТО БР ИББС-1.0-2010

Дата введения: 2010-06-21

Издание официальное

СТО БР ИББС

- ✓Положения объединили в себе рекомендации из писем Банка России
- ✓Появились новые требования, например к ТЗ
- ✓Механизмы информирования клиентов об операциях
- ✓Требования к документарному обеспечению функционирования ДБО
- ✓Приоритет «толстому» клиенту
- ✓Требования по оценке рисков
- ✓Требование к регистрацию операций при осуществлении ДБО

Общая структура нормативных документов

161 – ФЗ
О национальной платежной системе

115-ФЗ
О противодействии легализации …

152 – ФЗ
О персональных данных

…

382 - П

2831-У

Письма Банка России

СТО БР ИББС

Методические рекомендации НП «НПС», АРБ

Значимые статьи №161-ФЗ с точки зрения ИБ

- Статья 3. Основные понятия, используемые в настоящем Федеральном законе
- **Статья 9. Порядок использования электронных средств платежа**
- Статья 20. Правила платежной системы
- Статья 26. Обеспечение банковской тайны в платежной системе
- Статья 27. Обеспечение защиты информации в платежной системе
- Статья 28. Система управления рисками в платежной системе

Вехи по безопасности

- ✓ *В случае хищения денежных средств со счета клиента банк обязан возместить полную сумму похищенных средств* (Закон о национальной платежной системе, статья 9 пп. 11-16, вступает в силу с 1 января 2014 года)

Возможные поправки в ГК РФ

Статья 856.1. Риск убытков банка и клиента-гражданина при использовании электронного средства платежа

...

4. В случае, если банк исполнил обязанность по информированию клиента о совершении операции с использованием электронного средства платежа, а клиент уведомил банк по правилам пункта 7 статьи 847 настоящего Кодекса, клиент несет риск убытков от совершения такой операции до момента направления банку уведомления, предусмотренного пунктом 7 статьи 847 настоящего Кодекса, в размере не более десяти процентов от суммы денежных средств, списанных при совершении операции с использованием электронного средства платежа, если докажет одно из следующих обстоятельств:

1) **клиент лишился электронного средства платежа не по своей воле;**

2) **направление уведомления клиентом в срок**, указанный в пункте 7 статьи 847 настоящего Кодекса, **было невозможно по причинам, не зависящим от клиента**;

3) **в момент совершения операции с использованием электронного средства платежа клиент не находился и не мог находиться в месте совершения операции или не утратил владения электронным средством платежа.**

5. **Банк обязан по требованию клиента предоставить клиенту все имеющиеся у банка доказательства**, подтверждающие наличие обстоятельств, указанных в пункте 4 настоящей статьи, а также запросить такие доказательства у третьих лиц.

Общая структура нормативных документов

161 – ФЗ
О национальной платежной системе

115-ФЗ
О противодействии легализации …

152 – ФЗ
О персональных данных

…

382 - П

2831-У

Письма Банка России

СТО БР ИББС

Методические рекомендации НП «НПС», АРБ

382-П. Предмет документа

- Так, к защищаемым относятся сведения об остатках денежных средств на банковских счетах, а также электронных денег; о совершенных переводах денежных средств; о платежных клиринговых позициях. Речь идет и об информации, необходимой для удостоверения клиентами права распоряжения деньгами, а также ограниченного доступа, подлежащей обязательной защите и др.
- Приложение к документу содержит:
  - Порядок проведения оценки соответствия и документирования ее результатов **(напоминает методику оценки соответствия СТО БР ИББС)**
  - Форма 1. Документирование результатов оценки соответствия
  - Форма 2. Документирование результатов вычислений обобщающих показателей выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств
  - Перечень требований к обеспечению защиты информации при осуществлении переводов денежных средств, выполнение которых проверяется при проведении оценки соответствия

Требования применимые к ДБО

- ✓ Регистрация действий клиентов
- ✓ Регистрация действий с назначением и распределением прав клиентов
- ✓ Обеспечение возможности приостановить (блокировать) самим клиентом прием к исполнению его распоряжения
- ✓ Применение организационных и технических мер защиты информации
- ✓ Снижение тяжести последствий от воздействия с целью невозможности предоставления услуг
- ✓ Информирование клиентов
- ✓ Обеспечение сохранности информации о переводах
- ✓ Сверка выходных и входных электронных сообщений
- ✓ Выявление фальсифицированных электронных сообщений
- ✓ Полное документальное обеспечение безопасности переводов
- ✓ Анализ рисков
- ✓ Регулярная отчетность по инцидентам и оценке соответствия 382-П

2831-У. Предмет документа

- Установлены формы отчетности по обеспечению защиты информации при осуществлении переводов денежных средств:
  - операторами платежных систем,
  - операторами услуг платежной инфраструктуры,
  - операторами по переводу денежных средств
- Определены сроки предоставления и методики составления.
- **Сведения о выполнении операторами требований к обеспечению защиты информации** подаются по форме 0403202.
- **Сведения о выявлении инцидентов, связанных с нарушением требований**, подаются по форме 0403203.

Форма 0403202

Сведения о выполнении операторами платежных систем, операторами услуг платежной инфраструктуры, операторами по переводу денежных средств требований к обеспечению защиты информации при осуществлении переводов денежных средств

по состоянию на "__" _____ ____ г.

Наименование _____

Почтовый адрес _____

Код формы по ОКУД 0403202

На нерегулярной основе

I	Вид деятельности	
II	Регистрационный номер оператора платежной системы	
III	Предоставление услуг платежной инфраструктуры	
IV	Участие в платежных системах	

Номер строки	Вид сведений	Содержание
1	2	3
Сведения о выполнении требований к обеспечению защиты информации при осуществлении переводов денежных средств		
1	Показатель EV1 ПС	
2	Показатель EV2 ПС	
3	Итоговый показатель R ПС	
Сведения об оценке выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств		
4	Проведение оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств	

Руководитель
(заместитель руководителя) _____ _____
(личная подпись) (инициалы, фамилия)

М.П.

Исполнитель _____ _____
(личная подпись) (инициалы, фамилия)

Номер телефона:

Форма 0403203

Сведения о выявлении инцидентов, связанных
с нарушением требований к обеспечению защиты информации
при осуществлении переводов денежных средств

по состоянию на "__" _____ ____ г.

Наименование _____
Почтовый адрес _____

Код формы по ОКУД 0403203

Месячная

Количество инцидентов (единицы) _____

Номер строки	Дата выявления инцидента	Наименование банковского платежного агента (субагента)	Код банковского платежного агента (субагента) по ОКПО	Регистрационные номера операторов платежных систем	Последствия инцидента	Объекты информационной инфраструктуры	Описание предпринятых действий по устранению последствий инцидента	Факт обращения в правоохранительные органы
1	2	3	4	5	6	7	8	9

Руководитель
(заместитель руководителя) _____ _____
(личная подпись) (инициалы, фамилия)

М.П.

Исполнитель _____ _____
(личная подпись) (инициалы, фамилия)

Общая структура нормативных документов

161 – ФЗ
О национальной платежной системе

115-ФЗ
О противодействии легализации …

152 – ФЗ
О персональных данных

…

382 - П

2831-У

Письма Банка России

СТО БР ИББС

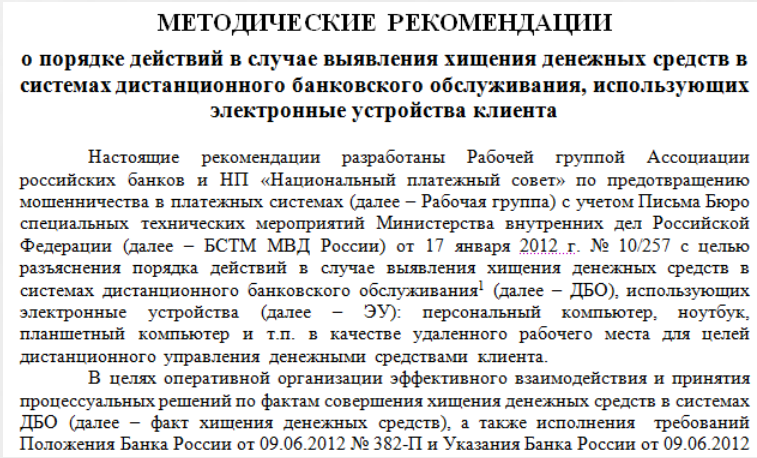
Методические рекомендации НП «НПС», АРБ

Методические рекомендации НП «НПС», АРБ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента

- ✓Действия клиента – юридического лица
- ✓Действия клиента – физического лица
- ✓Действия банк плательщика
- ✓Действия банка получателя

14 приложений (формы документов, перечни документов, образцы писем)



МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента

Настоящие рекомендации разработаны Рабочей группой Ассоциации российских банков и НП «Национальный платежный совет» по предотвращению мошенничества в платежных системах (далее – Рабочая группа) с учетом Письма Бюро специальных технических мероприятий Министерства внутренних дел Российской Федерации (далее – БСТМ МВД России) от 17 января 2012 г. № 10/257 с целью разъяснения порядка действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания[1] (далее – ДБО), использующих электронные устройства (далее – ЭУ): персональный компьютер, ноутбук, планшетный компьютер и т.п. в качестве удаленного рабочего места для целей дистанционного управления денежными средствами клиента.

В целях оперативной организации эффективного взаимодействия и принятия процессуальных решений по фактам совершения хищения денежных средств в системах ДБО (далее – факт хищения денежных средств), а также исполнения требований Положения Банка России от 09.06.2012 № 382-П и Указания Банка России от 09.06.2012

МОСКОВСКИЙ ГОРОДСКОЙ СУД

ОПРЕДЕЛЕНИЕ
от 2 февраля 2012 г. по делу N 33-3013

Судья Колмыкова И.Б.

Судебная коллегия по гражданским делам Московского городского суда в составе председательствующего Строгонова М.В.,
судей Шубиной И.И. и Мухортых Е.Н.,
при секретаре П.,
заслушав в открытом судебном заседании по докладу судьи Мухортых Е.Н. дело по кассационной жалобе М. на решение Тушинского районного суда г. Москвы от *** года, которым постановлено:
В удовлетворении исковых требований *** к ОАО "***" о взыскании денежных средств, компенсации морального вреда, взыскании судебных расходов отказать,

установила:

М. обратилась в суд с иском к ОАО "***", просила взыскать с ответчика в свою пользу денежные средства в размере *** руб., компенсацию морального вреда в размере ***руб., расходы на оплату услуг представителя в размере *** руб. В обоснование заявленных требований М. указала о том, что она является владельцем карты *** Master Card ***, выданной подразделением *** на основании договора N *** от *** г. С указанной карты *** г. без ведома истца были списаны тремя переводами на неизвестные ей счета денежные средства на общую сумму *** руб. При этом сама карта находилась у истца. В службе технической поддержки банка карту заблокировали. *** г. истец обратилась в отделение *** с заявлением о несанкционированном списании денежных средств. В отделении банка истца уверили в том, что списание денежных средств произошло вследствие технической неисправности и они будут ей возвращены. Однако до настоящего времени деньги истцу не возвращены. *** г. истец направил в адрес ответчика претензию с требованием возврата денежных средств. На данную претензию ответ получен не был. *** г. при получении выписки из лицевого счета по вкладу истец узнал, что денежные средства, с учетом комиссии, были фактически списаны с лицевого счета истца *** г., т.е. через 3 дня после получения банком сообщения о несанкционированных операциях и через 2 дня после обращения в отделение банка с заявлением о незаконных операциях по банковскому счету и блокировки карты.

*** г. М. обратилась в ОВД по району *** г. Москвы с заявлением по факту снятия денежных средств с банковской карты ОАО "***". В ходе проверки по данному заявлению ОВД установил, что ***г. М., находясь по месту жительства, пользовалась услугами интернета на сайте "***", производила операции по оплате коммунальных услуг. В это время на ее мобильный телефон поступило смс-сообщение о том, что с ее карты сняты денежные средства в сумме *** руб. Ответ на запрос из службы безопасности до окончания срока проверки о том, где были обналичены денежные средства, получен не был. Документальных подтверждений о том, что данная сумма денег была снята со счета М., также не имеется. Постановлением УУМ ОВД по району *** г. Москвы от *** г. в возбуждении уголовного дела отказано за отсутствием события преступления.

В судебном заседании специалист *** пояснила, что идентификатор и постоянный пароль для входа в систему "***" был получен М. самостоятельно с введением ПИН-кода через банкомат. *** г. М. вошла в систему, вход был подтвержден паролем и идентификатором, и провела три операции по переводу денежных средств. Данные операции были подтверждены одноразовыми паролями, переданными банком М. на ее личный мобильный телефон. Все финансовые операции подтверждаются паролями, без которых денежные средства с карты не могут быть списаны. В смс-сообщении банка указывается и текст операции, т.е. к какой операции предоставлен данный пароль. По результатам проведенного службой безопасности банка расследования выяснилось, что персональный компьютер М. был заражен вирусом, действие которого проявляется в том, что при входе на сайт ОАО "***" вирус перенаправлял клиента на сайт, имитирующий сайт ОАО "***". Одновременно мошенники, которые заразили персональный компьютер, входили на оригинальный сайт ОАО "***". При проведении операций мошенники направили запрос в банк на получение паролей, в ответ на который ОАО "***" направил ответ на мобильный телефон клиента. А клиент, не сравнив информацию о параметрах операции, в своем персональном компьютере ввел данный пароль на сайте, имитирующем сайт ОАО "***", в связи с чем он стал доступен мошенникам. Они его подтвердили и деньги были списаны с карты истца.

Выводы и решение суда

- Подписав заявление на получение международной дебетовой карты Master Card Standart, М. согласилась с "Условиями использования международных карт России ОАО", а именно: не сообщать ПИН-код и не передавать карту (ее реквизиты) для совершения операций другими лицами, предпринимать необходимые меры для предотвращения утраты, повреждения, хищения карты, нести ответственность по операциям, совершенным с использованием ПИН-кода.
- Действия истца М. по использованию банковской карты ОАО "***" нельзя признать добросовестными, поскольку она надлежащим образом принятые на себя обязательства по договору не исполнила. Истец М. как клиент ОАО "***" должна была осознавать возможность наступления рисков, связанных с операциями, проводимыми через систему "***", "Мобильный банк". В связи с этим суд первой инстанции посчитал, что в данном случае ответственность за причиненный истцу ущерб, возникший вследствие несанкционированного использования третьими лицами средств подтверждения клиента, если такое использование стало возможно не по вине банка, не может быть возложена на ответчика.
- С утверждениями истца в кассационной жалобе о том, что доводы специалиста *** о том, что компьютер истца был заражен вирусом, являются недостоверными, т.к. осмотр компьютера не производился, судебная коллегия согласиться не может. То обстоятельство, что компьютер истца не был обследован специалистами, с учетом имеющихся в банке технических средств и информационных ресурсов, консультацию специалиста не опровергает.
- Доводы кассационной жалобы о том, что в *** г. при входе в систему "***" истец подтверждения об этом от банка не получил, являются голословными и ничем не подтверждены. Судом установлено, что истцу оказывается услуга смс-оповещение, которая предусматривает предоставление клиенту информации обо всех совершаемых по счетам карт операциях путем немедленной передачи сообщения на мобильный телефон, указанный клиентом. Претензий к качеству указанной услуги от М. не поступало.

Коллеги,
Большое спасибо за внимание!

Web: http://www.tsarev.biz/
Twitter: http://twitter.com/TsarevEvgeny
Facebook: http://www.facebook.com/tsarev.biz
E-mail: TsarevEO@gmail.com
Tel: +7-926-104-70-58