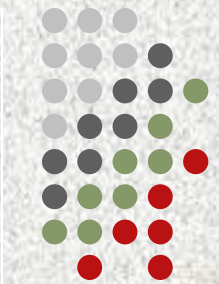
V Юбилейный Уральский форум
«Информационная безопасность банков»

ПОДХОДЫ К ПРОВЕДЕНИЮ ПРОВЕРОК КРЕДИТНЫХ ОРГАНИЗАЦИЙ ПО ВОПРОСАМ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Сергей Николаевич Стройков,
Главная инспекция кредитных организаций Банка России

Основные направления проверки



При проведении проверки кредитной организации по вопросам применения информационных технологий (ИТ) основное внимание уделяется **организации и осуществлению**:

- **управления информационными потоками (получением и передачей информации);**
- **обеспечения информационной безопасности (ИБ);**
- **функционирования системы управления банковскими рисками, связанными с применением ИТ.**

В ходе проверки формируются:

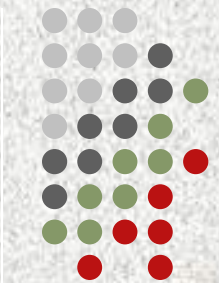
- **Оценка организации внутреннего контроля за применением ИТ в кредитной организации**

(согласно Положению Банка России от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах», разработанному на основании ст. 57 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»);

- **Оценка соблюдения требований к обеспечению защиты информации при осуществлении переводов денежных средств**

(согласно Положению Банка России от 09.06.2012 № 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», разработанному на основании ст. 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»).

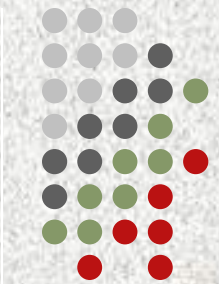
а также осуществляется контроль достоверности отчетности:



- **По форме 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 форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств».**

(согласно Указанию Банка России от 09.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств»)

Проверка организации внутреннего контроля за применением ИТ предусматривает:



I. **Оценку внутренних документов, регламентирующих организацию внутреннего контроля за применением ИТ;**

II. **Оценку осуществления контроля со стороны органов управления кредитной организации за организацией деятельности в части применения ИТ;**

III. **Оценку деятельности службы внутреннего контроля кредитной организации (СВК) в части осуществления контроля за применением ИТ;**

IV. **Оценку осуществления внутреннего контроля за управлением информационными потоками (получением и передачей информации) и обеспечением ИБ;**

V. **Оценку осуществления внутреннего контроля за функционированием системы управления банковскими рисками в кредитной организации, связанными с применением ИТ, и оценку банковских рисков, связанных с применением ИТ.**

В целях контроля соблюдения требований к обеспечению защиты информации при осуществлении переводов денежных средств Банк России в том числе проводит:

- **проверки кредитных организаций (выступающих в качестве операторов платежных систем, операторов услуг платежной инфраструктуры и операторов по переводу денежных средств)**

(в соответствии с порядком, установленным Инструкцией Банка России от 25.08.2003 № 105-И «О порядке проведения проверок кредитных организаций (их филиалов) уполномоченными представителями Центрального банка Российской Федерации»);

- **инспекционные проверки иных (не кредитных) организаций (выступающих в качестве операторов платежных систем и операторов услуг платежной инфраструктуры**

(в соответствии с порядком, установленным Банком России на основании Федерального закона № 161-ФЗ);

Состав требований к обеспечению защиты информации при осуществлении переводов денежных средств:

I. Требования к обеспечению защиты информации при осуществлении переводов денежных средств:

1) применяемые для защиты информации:

- при назначении и распределении функциональных прав и обязанностей (ролей) лиц, связанных с осуществлением переводов денежных средств;
- на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры;
- при осуществлении доступа к объектам информационной инфраструктуры, в том числе от несанкционированного доступа;
- от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (вредоносный код);
- при использовании информационно-телекоммуникационной сети Интернет при осуществлении переводов денежных средств;
- при использовании СКЗИ;

2) с использованием взаимоувязанной совокупности организационных мер защиты информации и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры защиты информации);

Состав требований к обеспечению защиты информации при осуществлении переводов денежных средств:

II. Требования к организации и функционированию подразделения (работников), ответственного (ответственных) за организацию и контроль обеспечения защиты информации (служба информационной безопасности);

III. Требования к повышению осведомленности работников и клиентов в области обеспечения защиты информации;

IV. Требования к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагированию на них;

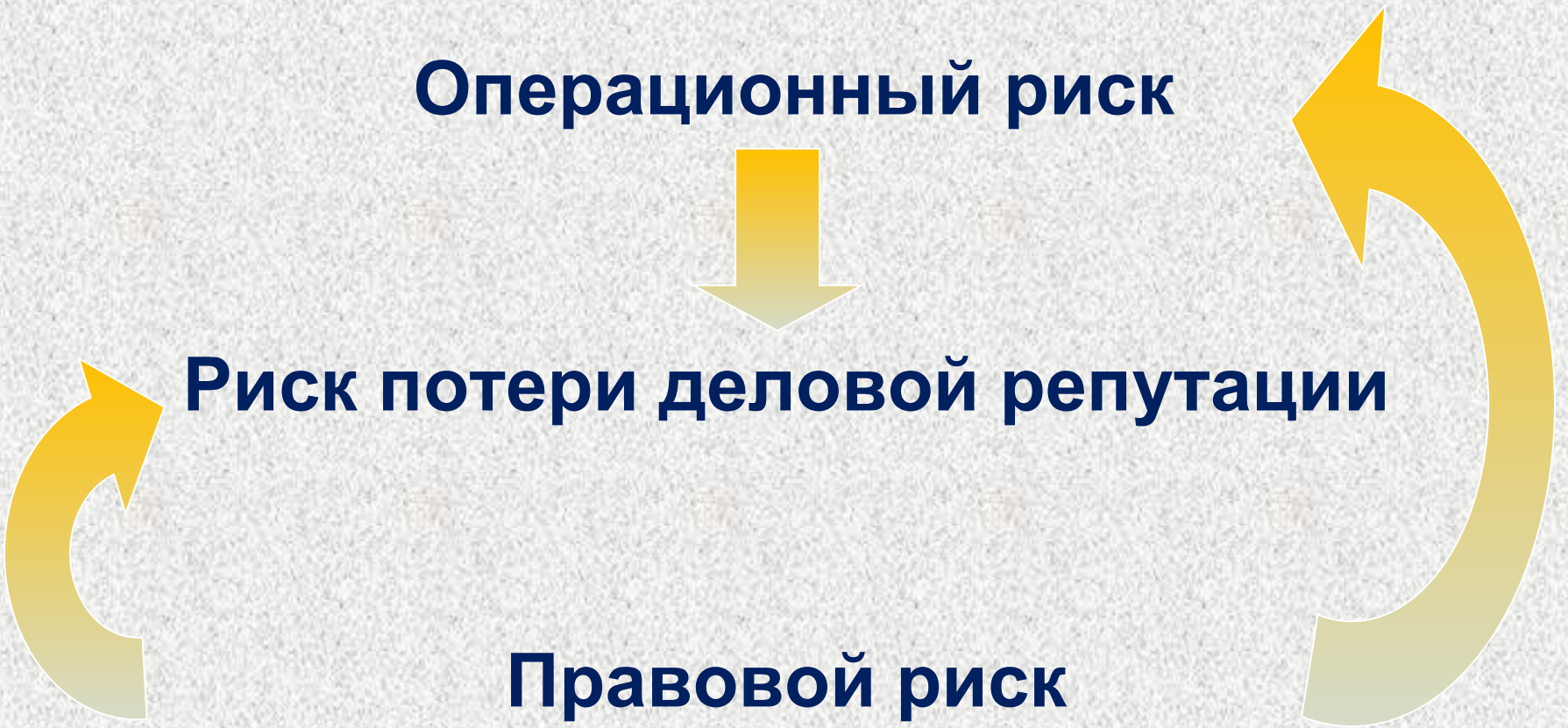
V. Требования к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;

VI. Требования к оценке выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств;

VII. Требования к доведению оператором по переводу денежных средств, оператором услуг платежной инфраструктуры до оператора платежной системы информации об обеспечении в платежной системе защиты информации при осуществлении переводов денежных средств;

VIII. Требования к совершенствованию защиты информации при осуществлении переводов денежных средств.

К основным банковским рискам, связанным с применением ИТ, относятся:



При проверке функционирования системы управления банковскими рисками, связанными с применением ИТ, рассматриваются:

I. **в случае не использования услуг сторонних организаций в сфере ИТ**:

- применяемые методы выявления и оценки банковских рисков, связанных с применением ИТ*;*
- наличие определения влияния на размер банковских рисков, связанных с применением ИТ, составляющих информационной инфраструктуры кредитной организации;
- наличие моделей угроз и нарушителей, связанных с применением ИТ;
- наличие установленного порядка постоянного наблюдения (мониторинга) за размером банковских рисков, связанных с применением ИТ;
- принимаемые меры по поддержанию банковских рисков, связанных с применением ИТ, на не угрожающем финансовой устойчивости кредитной организации и интересам ее кредиторов и вкладчиков уровне;
- осуществление контроля со стороны органов управления кредитной организации за управлением банковскими рисками, связанных с применением ИТ, и их оценкой.

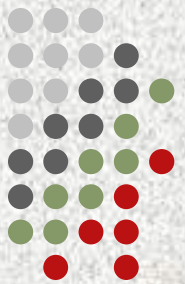
При проверке функционирования системы управления банковскими рисками, связанными с применением ИТ, рассматриваются:

II. при использовании услуг сторонних организаций в сфере ИТ:

- **мероприятия по управлению банковскими рисками, связанными с применением ИТ, при использовании услуг сторонних организаций в сфере ИТ;**
- **содержание условий договоров (контрактов) со сторонними организациями на оказание услуг в сфере ИТ, касающихся случаев возникновения конфликтных ситуаций и непредвиденных (чрезвычайных) обстоятельств;**

Договоры (контракты) кредитной организации (её филиала) со сторонними организациями на оказание услуг в сфере ИТ могут предусматривать как предоставление кредитной организации внешних информационных ресурсов и сервисов, так и предоставление информационных ресурсов и сервисов кредитной организации клиентам и/или другим внешним потребителям (при этом в договоре могут участвовать две, три или более сторон).

В рамках контроля кредитных организаций по вопросам применения ИТ



В период с 2009 по 2012 годы ежегодно в среднем при проведении **20%** плановых проверок Банком России рассматривались вопросы применения кредитными организациями ИТ.

Типичными недостатками, выявляемыми Банком России в ходе проверок кредитных организаций по вопросам применения ИТ, являются:

- ***Отсутствие*** *политики применения и развития ИТ.*
- ***Несоответствие*** *политики применения и развития ИТ характеру, условиям и масштабам деятельности кредитной организации.*
- ***Несоблюдение*** *требований внутренних документов кредитной организации по вопросам применения ИТ.*
- ***Несоответствие*** *планов действий на случай нештатных ситуаций условиям деятельности кредитной организации.*

СПАСИБО ЗА ВНИМАНИЕ

Сергей Николаевич Стройков,
Главная инспекция кредитных организаций Банка России