Банк России
Центральный банк Российской Федерации

Перспективы развития регулирования операционных рисков в части киберрисков

Бухтин М.А.
Начальник Управления моделирования рисков
Департамент банковского регулирования (ДБР)

Доклад на X Уральском форуме Информационной безопасности финансовой сферы

15 Февраля 2018

Банк России
Центральный банк Российской Федерации

Банковское регулирование операционных рисков в части киберрисков

Понятие операционного риска

Операционный риск (ОР) – это риск прямых или косвенных потерь в результате:

- **неадекватных или ошибочных внутренних процессов**
- действий сотрудников
- нарушение штатной работы систем
- внешних событий

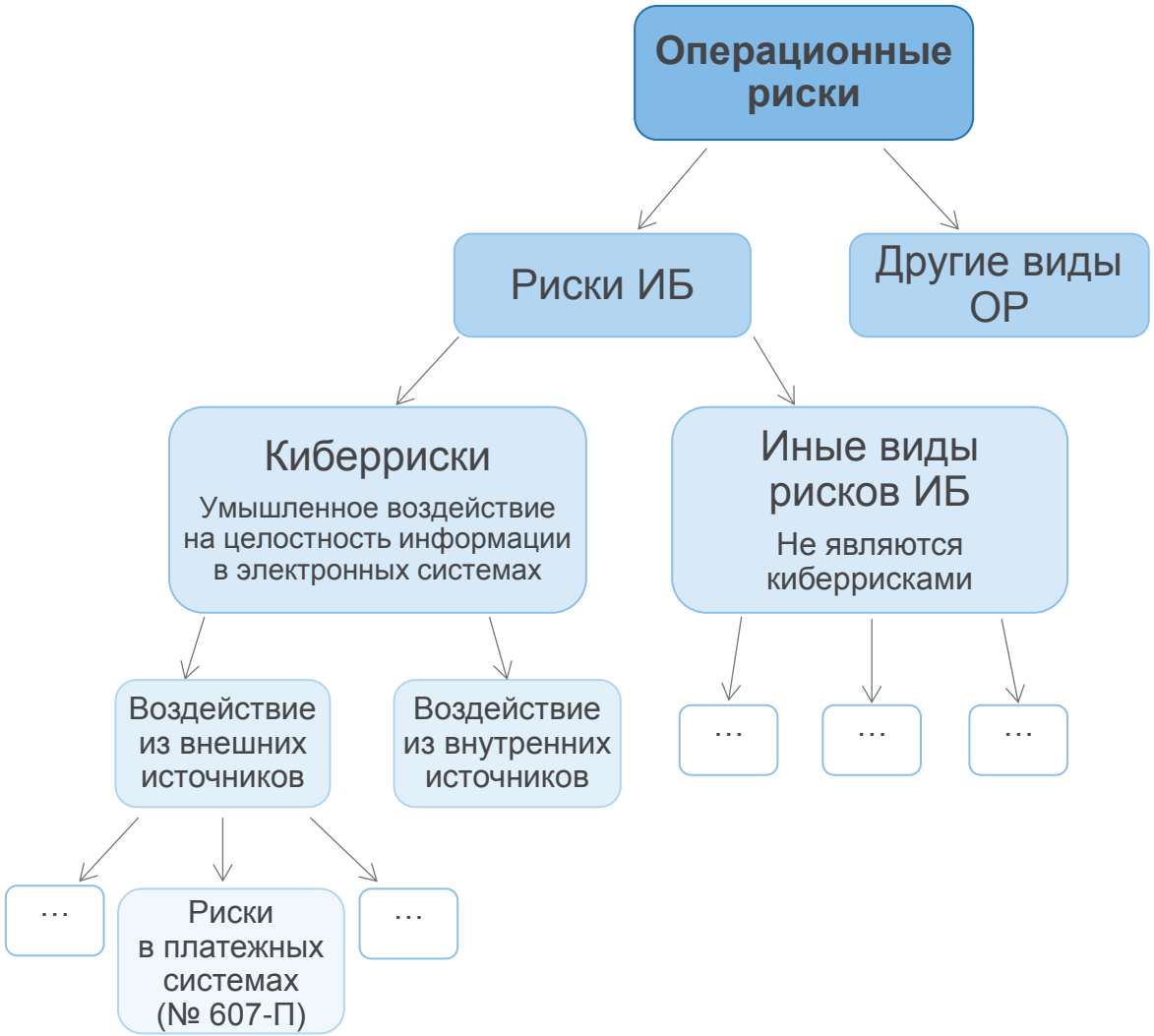
ОР включает в себя юридический риск, но не включает стратегический и репутационный риски

В ОР входят разные виды рисков в зависимости **от видов процессов**:

- **риски информационной безопасности (ИБ)**
- кадровые риски
- риски недостатков внутреннего контроля
- ИТ-риски
- риски проектов
- риски ОНиВД*

* ОНиВД – обеспечение непрерывности и восстановления деятельности кредитной организации

Структура рисков информационной безопасности (ИБ) с точки зрения банковского регулирования ОР



Особенности управления отдельными видами ОР

Отдельные виды ОР могут управляться специализированным подразделением (не обязательно службой анализа рисков)

Основная особенность управления ОР: децентрализованность управления отдельными видами ОР, в том числе на основе своих специализированных стандартов, например, рисками ИБ (киберрисками)

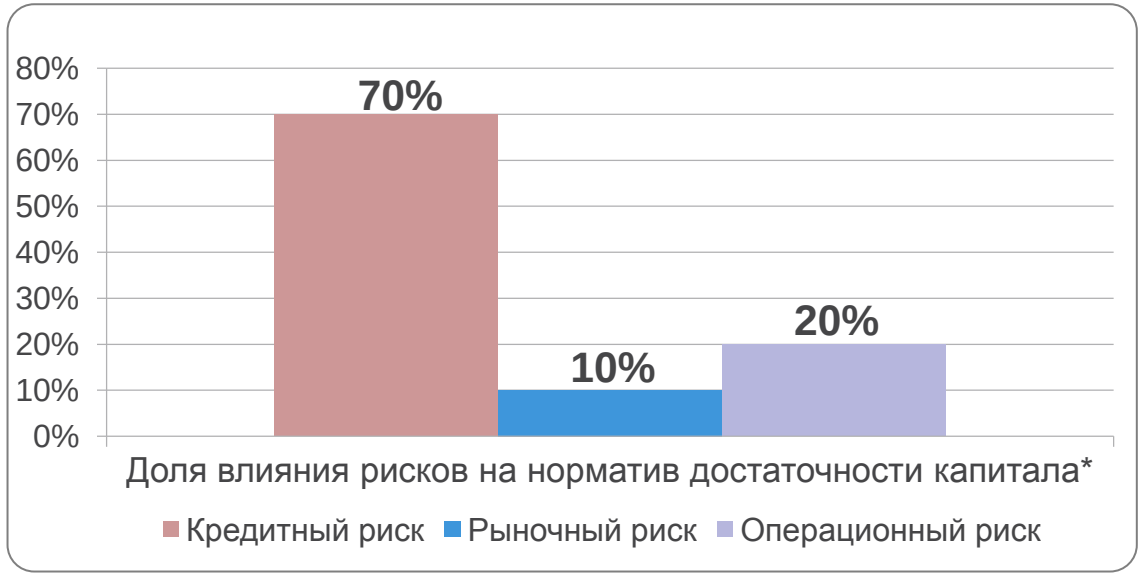
Задачи банковского регулирования

- формализация **единых** требований к качеству систем управления операционными рисками
- адекватная оценка возможных потерь от ОР для целей выделения на них фондов покрытия потерь (регуляторного и экономического капитала)

Место операционного риска в нормативе достаточности капитала

Основной способ банковского регулирования ОР – требование на выделение капитала на покрытие совокупных потерь от ОР в рамках Инструкции Банка России № 180-И (Положения Банка России № 346-П):

$$\mathrm{H}_1 = \frac{K_i}{\underbrace{[\text{Кредит. риск}] + [\text{Рыночн. риск}] + [OP]}_{RWA}}$$



Все требования к расчету RWA соответствуют стандартам Базель II и не могут быть пересмотрены Банком России без учета данных стандартов

Например, киберриск **не** может быть включен как отдельный элемент в состав RWA. В соответствие с этим, капитал на покрытие потерь на киберриск рассчитывается в составе ОР

* Экспертная оценка

Подходы к расчету величины капитала на ОР (Базель II)

- **Минимальный регуляторный капитал на ОР (180-И, 346-П):**

  Выделение базового индикатора, характеризующего объем операционной среды, который умножается на масштабирующий коэффициент потерь (α=15%), являющейся оценкой непредвиденных потерь с доверительной вероятностью 99%.

  Индикатор определяется на базе аналитических исследований зависимости индикатора от объема потерь. В настоящее время в качестве такого индекса выбран Gross Income (GI, Валовый доход)

- **Дополнительные требования к капиталу на ОР на основе базы данных о событиях ОР и возникших убытках (ВПОДК*, 3624-У):**

  Расчет величины требований к капиталу на основе накопленной статистики за 10 лет** и более (накопление данных продолжается на всем периоде жизни кредитной организации)

* ВПОДК – внутренние процедуры оценки достаточности капитала

** Базелем допускается начало использования статистики убытков в результате событий ОР, накопленной за меньший период, с последующим накоплением данных до 10 лет и далее

Планируемые изменения расчета величины капитала на ОР в рамках Базель III*

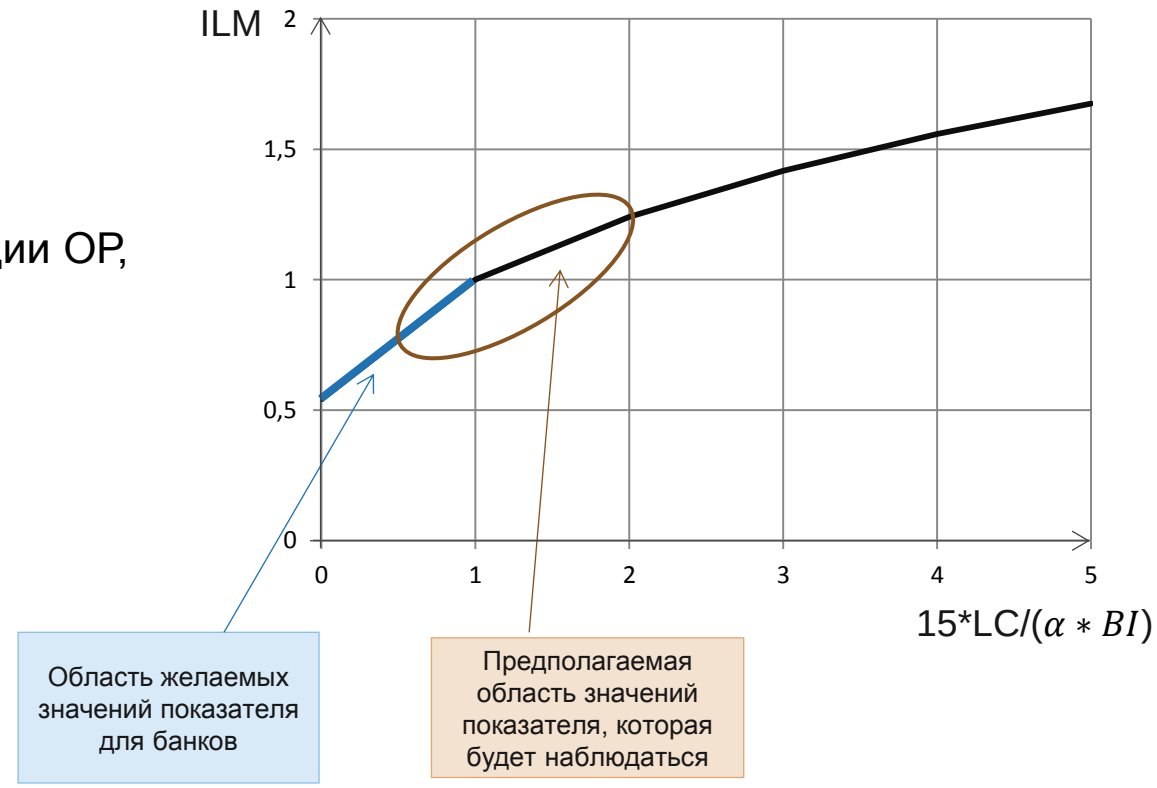
Изменение в подходе к оценке операционного риска: потери банка вследствие реализации ОР будут использоваться для расчета компоненты **Internal Loss Multiplier (ILM)**, включаемой в расчет величины капитала:

$$ILM = \ln(\exp(1) - 1 + \left(\frac{LC}{\alpha * BI}\right)^{0.8})$$

где Loss Component (LC) вычисляется как 15*среднее арифметическое годовых убытков вследствие реализации ОР, рассчитанное на временном горизонте 10 лет.

$$[\boldsymbol{OP}] = \boldsymbol{\alpha} * \boldsymbol{BI} * \boldsymbol{ILM}$$

где $\boldsymbol{\alpha}$ – 12%, 15% или 18% в зависимости от размера кредитной организации,
$\boldsymbol{BI}$ – бизнес-индикатор по аналогии с *Gross Income*



* Планируется к внедрению в 2021-2022 годах

Требования регуляторов к системе управления ОР*

В кредитной организации должна быть создана **база данных** о событиях ОР и убытках, понесенных вследствие реализации ОР, содержащая следующую информацию:

- размер убытков
- даты возникновения
- дата отражения убытка на балансе кредитной организации
- источник возникновения события (подразделение, автоматизированная система, наименование бизнес-процесса)
- поступившие возмещения
- информация о причинах и обстоятельствах возникновения событий

Назначение базы данных – контроль над уровнем фактически понесенных (прямых) убытков кредитной организации. В случае превышения среднегодовых потерь, рассчитанных на основе базы данных, над минимальным регуляторным капиталом устанавливается надбавка (буфер капитала)

Предусматривается классификация событий по:

- типам событий
- направлениям деятельности и составляющим их бизнес-процессах в разрезе структурных подразделений
- источникам событий
- видам убытков от событий возникновения операционного риска

ДБР планирует установить требования к отдельной классификации событий риска ИБ в составе БД ОР (в 2018 году)

* Формализуются в Указании Банка России № 3624-У в рамках ВПОДК. В последствие возможно издание отдельного нормативного акта.

Классификация событий ОР

По типам событий
- Внутреннее мошенничество
- Внешнее мошенничество
- Кадровая политика и безопасность труда
- Нарушения в клиентских продуктах и Деловой практики взаимодействия с клиентами
- Ущерб материальным (физическим) активам
- Нарушение функционирования и сбои систем
- Нарушения при организация, исполнение и управление процессами

По источникам ОР
- Неадекватные или ошибочные внутренние процессы
- Действия сотрудников
- Внешние события
- Сбой системы

Возможны дополнительные элементы классификации по видам риска

Событие ОР

По видам убытков
- Прямые убытки, как убытки, отраженные в виде прямых проводок по счетам расходов и (или) убытков в бухгалтерском учете кредитной организации
- Непрямые потери (не отраженные напрямую по счетам расходов и (или) убытков в бухгалтерском учете, но косвенно влияющих на финансовый результат) делятся на два вида:
  - ✓ косвенные потери (денежные потери, определяются расчетным способом)
  - ✓ качественные потери

Если у события ОР есть несколько источников, одним из которых связан с нарушениями процессов обеспечения ИБ, то такое событие ОР классифицируется как событие риска ИБ (при этом все остальные его источники сохраняются)

Дополнительные элементы классификации риска ИБ (см. следующий слайд)

По направлениям деятельности
- Корпоративное финансирование, включая муниципальное и государственное финансирование
- Операции и сделки на рынке ценных бумаг и срочных финансовых инструментов
- Розничное банковское обслуживание и частное банковское обслуживание
- Коммерческое банковское обслуживание корпоративных клиентов
- Платежи и расчеты
- Агентские услуги и кастодиальные услуги, депозитарий
- Управление активами
- Розничное брокерское обслуживание

Дополнительные элементы классификации риска ИБ

События риска ИБ		
Связанные **с переводами и платежами**	Возникшие в результате **несанкционированного доступа и (или) реализации компьютерных атак к объектам информационной инфраструктуры и (или) информационным системами** (в соответствие с ГОСТ Р 56546-2015)	Связанные с обработкой (хранением, уничтожением) информации **без использования средств автоматизации**
• возникшие в результате использования электронных средств платежа клиентов кредитных организаций без их согласия • связанные с переводами и снятиями денежных средств в результате несанкционированного доступа к объектам информационной инфраструктуры • возникшие в результате списания денежных средств с корреспондентских счетов участников платежной системы без их согласия и (или) с использованием искаженной информации • связанные с неоказанием кредитной организацией услуг по переводу денежных средств • возникшие в результате нарушений и недостатков обеспечения ИБ и управления рисками нарушения ИБ	• связанные с несанкционированным доступом к объектам информационной инфраструктуры и (или) информационным системами • возникшие в результате атак типа «отказ в обслуживании» (DDOS-атаки), предпринимаемых с целью блокирования нормального функционирования • возникшие в результате воздействия компьютерных вирусов • связанные с эксплуатацией уязвимостей в программном обеспечении информационных систем	• связанные с утечкой конфиденциальной информации • связанные с хищением или утратой носителей информации Возможны иные виды событий риска ИБ

! <u>Нерегулируемые вопросы:</u> расхождение в классификации видов рисков ИБ с точки зрения стандартов риск-менеджмента (банковское регулирование) и подходов к ИБ

Банк России
Центральный банк Российской Федерации

Требования в банковском регулировании к системе управления рисками ИБ (в составе требований к ОР)

В рамках ВПОДК планируется принять в 2018 г. (Указание № 3624-У)

Качественные требования к системе управления риском ИБ

Кредитная организация:

- определяет на плановый годовой период количественные и качественные показатели склонности к риску ОР, в том числе к риску ИБ (риск-аппетиты ОР и ИБ)
- устанавливает целевые уровни этих показателей: сигнальный (приемлемый) уровень и контрольный (лимитный) уровень

Расчет и обоснование сигнальных и контрольных значений показателей склонности к риску ИБ кредитная организация оформляет в виде мотивированного суждения и включает в состав материалов, выносимых на рассмотрение Совета директоров при утверждении стратегии управления рисками и капиталом

Качественные требования будут формулироваться в рамках ВПОДК в Указании Банка России № 3624-У ссылками на отраслевые стандарты ИБ (например, ГОСТР 57580.1-2017) с учетом качественных требований Базеля II к ВПОДК

Примеры показателей склонности к риску в части рисков ИБ

Вычисляются для кредитной организации за определенный период:

- **прямые убытки от реализации инцидентов ИБ** (за период) в разрезе:
  - убытки, связанные с операциями по переводу денежных средств (в платежных системах)*
    - ✓ суммы денежных средств, в отношении которой получены уведомления клиентов о переводе (списании) денежных средств с их банковских счетов в результате использования электронных средств платежа клиентов без их согласия
    - ✓ операционных расходов в результате использования электронных средств платежа клиентов без их согласия
    - ✓ операционных расходов в результате переводов и снятий денежных средств, связанных с несанкционированным доступом к объектам информационной инфраструктуры
    - ✓ операционных расходов в результате списания денежных средств с корреспондентских счетов участников платежной системы без их согласия и (или) с использованием искаженной информации, содержащейся в распоряжениях на перевод денежных средств
  - прямые убытки от иных инцидентов ИБ, не связанные с платежными системами
- **совокупные убытки от реализации инцидентов ИБ** (за период), включающей сумму прямых потерь и косвенных потерь

- $\frac{\text{сумма операционных расходов (убытков) при выполнении функций участника платежной системы Банка России}}{\text{общая сумма операций по переводу денежных средств через платежную систему Банка России}}$

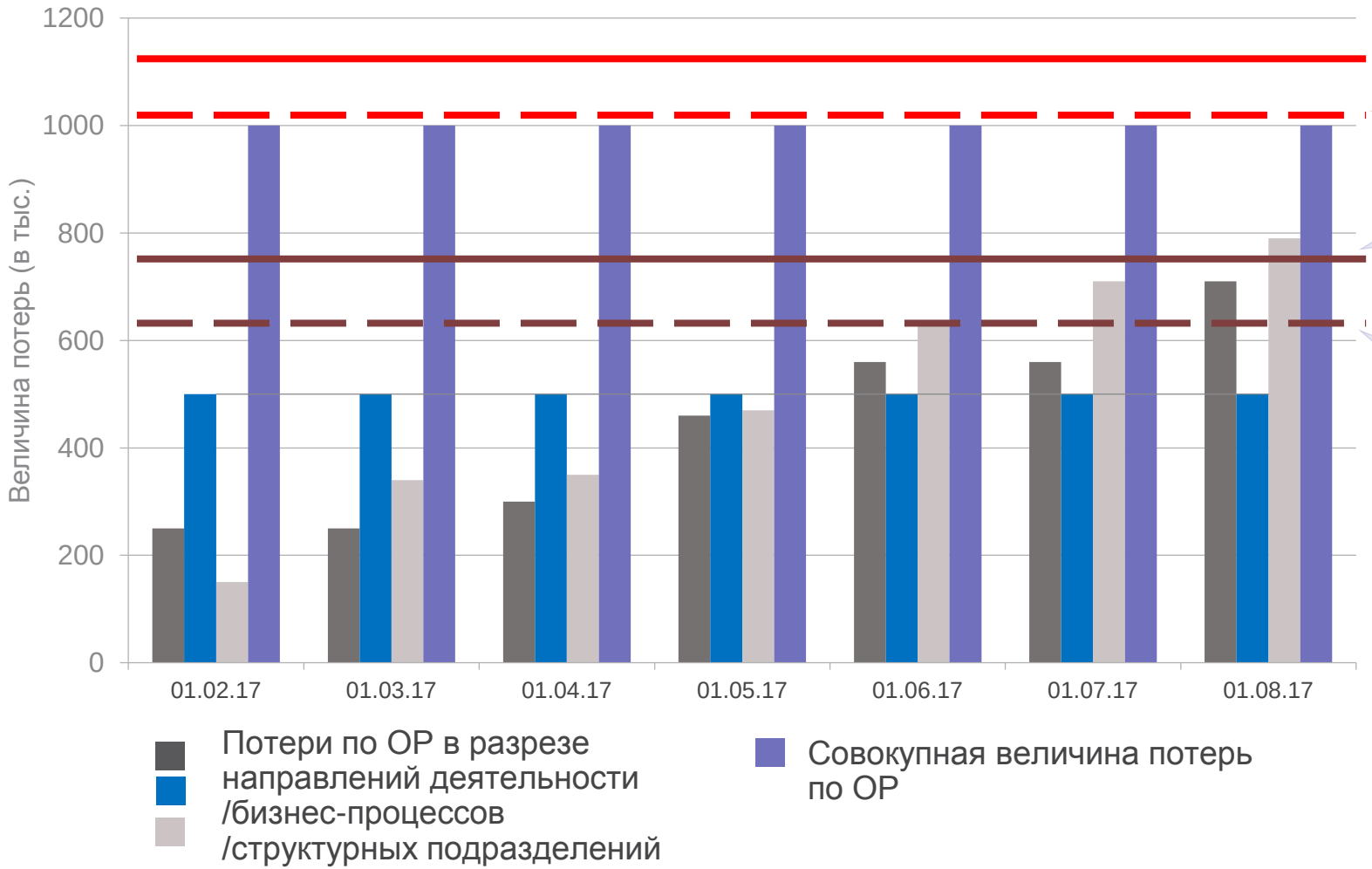
- $\frac{\text{сумма операционных расходов (убытков) при выполнении функций оператора иных платежных систем или оператора услуг платежной инфраструктуры}}{\text{общая сумма операций по переводу денежных средств через иные платежные системы или платежной инфраструктуры}}$

- $\frac{\text{сумма прямых убытков от реализации инцидентов ИБ}}{\text{общая сумма расходов (убытков)}}$

- $\frac{\text{сумма прямых убытков от реализации инцидентов ИБ (за годовой период)}}{\text{базовый капитал (на последнюю отчетную дату года)}}$

* ДБР берет за основу классификацию убытков по платежным операциям в соответствие с Федеральным законом № 161-ФЗ «О национальной платежной системе»

Контрольные и сигнальные значения показателей склонности к риску



Контрольный уровень совокупного риск аппетита по ОР

Сигнальный уровень совокупного риск аппетита по ОР

Контрольный уровень для риск аппетитов по направлениям деятельности / бизнес-процессам /структурным подразделениям

Сигнальный уровень для риск аппетитов по направлениям деятельности / бизнес-процессам /структурным подразделениям

Банк самостоятельно определяет уровни и утверждает их на Совете Директоров.

Уровни должны быть обоснованы и должны соотноситься с величиной минимального регуляторного капитала в рамках Положения № 346-П

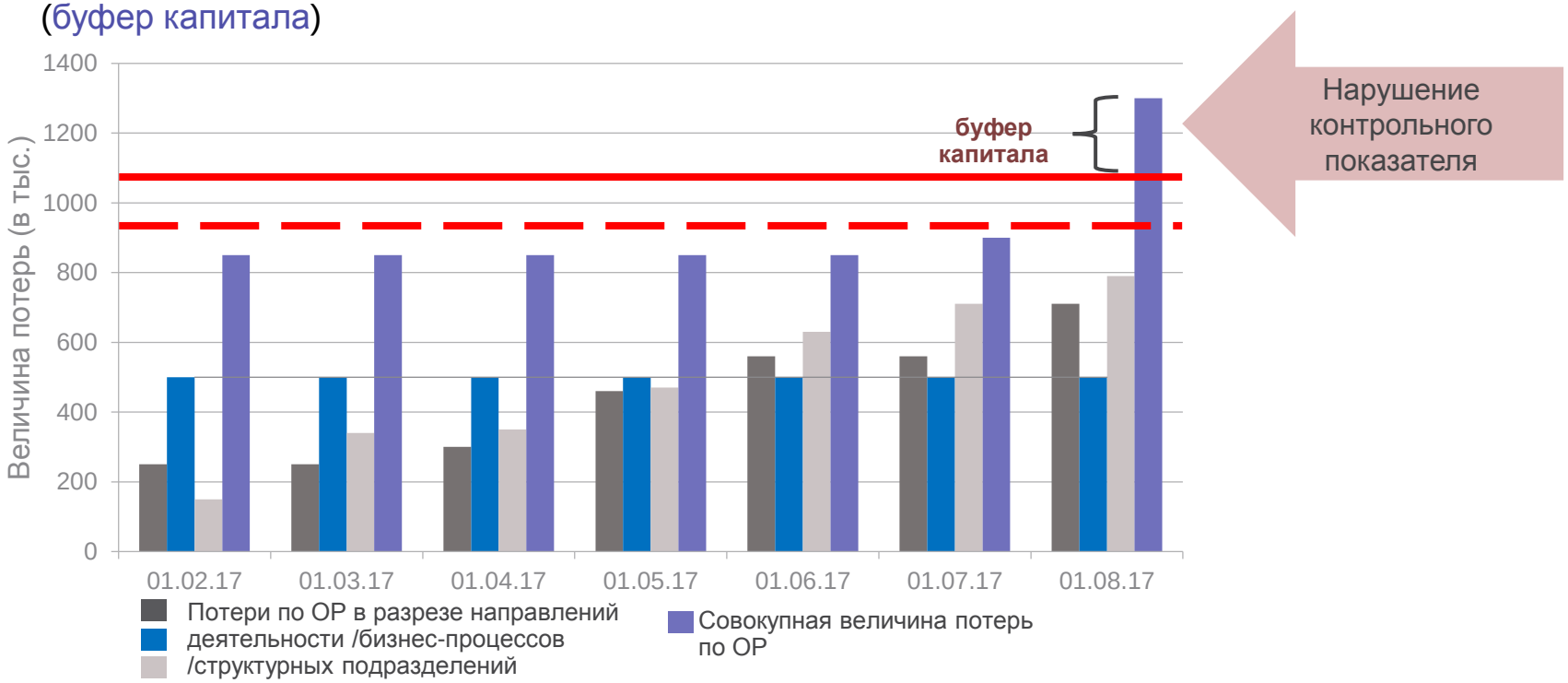
Количественные требования

1. Инструкции № 180-И предусматриваются количественные требования к величине минимального регуляторного капитала на покрытие операционного риска (на основе базового индикатора)

$$К_{мин\_регуляторн,ОР} = 15\% * GI$$

где *GI* – среднегодовой валовый доход

2. Согласно стандартам ВПОДК (№ 3624-У, № 3883-У) в случае, если кредитная организация нарушает контрольный показатель склонности к риску, установленный в СУРиК, банку назначаются дополнительные требования к капиталу сверх регуляторных (буфер капитала)



Банк России
Центральный банк Российской Федерации

Контроль за системой управления ОР

Контроль за системой управления ОР и рисками ИБ

Контроль осуществляется с помощью:

- регулярного составления отчетности и ее рассмотрения органами управления кредитной организацией
- самооценки соответствующих подразделений
- оценки, проводимой внешней организацией (внешний аудит)
- проверок Службы внутреннего аудита
- надзорной оценки со стороны Банка России, включая оценку качества системы ИБ и защиты данных

Отчеты по результатам контроля:

- рассматриваются Наблюдательным советов и Советом Директоров кредитной организации
- направляются в подразделение банковского надзора Банка России с последующим принятием решения по результатам их рассмотрения

Внутренняя отчетность в рамках контроля за системой управления ОР и рисками ИБ

Внутренняя отчетность кредитной организации по ОР должна включать информацию о событиях реализации ОР в разрезе направлений деятельности, типов событий, источникам риска по следующим показателям (с начала года до отчетной даты и в отчетном периоде), **например:**

- общее количество событий, которые были зафиксированы у кредитной организации
- количество событий, принесших убытки кредитной организации, которые отразились на балансовых счетах кредитной организации
- сумма прямых убытков, которые отразились на балансовых счетах кредитной организации
- максимальный убыток от одного события из тех, которые были зафиксированы у кредитной организации
- максимальная сумма убытков от пяти событий из тех, которые были зафиксированы у кредитной организации
- сумма непрямых расчетных убытков, которые могли быть и возможно будут в будущих периодах у кредитной организации в результате события реализации ОР, в части упущенной выгоды, сорванных сделок, штрафных санкций и т.д.
- сумма непрямых убытков, которые были у кредитной организации в результате события реализации ОР, в части восстановления оборудования, выплаты компенсаций, заказа услуг по восстановлению третьих лиц и т.д.
- сумма возмещенных убытков, которые отразились на балансовых счетах кредитной организации
- консолидированная сумма убытков с учетом суммы возмещения, которые были отражены на балансовых счетах кредитной организации
- среднеквадратичное отклонение (сигма) величины убытков от событий реализации ОР

Надзорная оценка системы управления ОР и рисками ИБ (1/3)

№ п/п	Параметры оценки	Вес	Баллы
1	Оценка подверженности банка операционному риску	2	
2	Оценка процедуры выявления, измерения и ограничения операционного риска	3	
3	Оценка уровня достаточности капитала на покрытие операционного риска в соответствии с требованиями, установленными нормативными актами Банка России	3	
4	Соблюдение приемлемого уровня операционных расходов (убытков) в результате несанкционированного доступа к объектам ее информационной инфраструктуры, используемой для осуществления переводов денежных средств, или в результате использования электронных средств платежа без согласия клиентов*	3	
5	Оценка уровня защиты информации в соответствии с требованиями, установленными нормативными актами Банка России*	3	

* Планируемые изменения в рамках Указаний № 4336-У и 3883-У (в 2018 г.)
Будут дополнительно определены соответствующие критерии для выставления оценок. Также в части п.5 будет решаться вопрос относительно того, кто является субъектом оценки (куратор/надзорное подразделение/внешняя организация)

Надзорная оценка системы управления ОР и рисками ИБ (2/3)

Показатель оценки операционного риска (ПООР) и показатель оценки риска информационной безопасности (ПРИБ) представляют собой средние взвешенные значения оценок ответов на вопросы и рассчитываются:

$$\text{ПООР, ПРИБ} = \sum_{i=1}^{n} (\text{балл}_i \times \text{вес}_i) : \sum_{i=1}^{n} \text{вес}_i,$$

где *балл*$_i$ - оценка от 1 до 4 ответа на соответствующий вопрос, приведенный в таблицах Приложения 5 к настоящему Указанию (балльная оценка);

вес$_i$ - оценка по шкале относительной значимости от 1 до 3 ответа на соответствующий вопрос, приведенный в таблицах соответствующего проекта нормативного акта

n - количество вопросов в таблицах показателя оценки операционного риска (ПООР) и показателях оценки риска информационной безопасности (ПРИБ)

Надзорная оценка системы управления ОР и рисками ИБ (3/3)

Результатом надзорной оценки является отнесение системы управления ОР кредитной организации к одной из групп качества ВПОДК (где 1 – наилучшая оценка, 5 – наихудшая оценка)
(Указание Банка России № 3883-У)

Классификационная группа, определенная в соответствии с Указанием Банка России № 4336-У / Оценочная категория качества ВПОДК, определенная в соответствии с главой 2 Указания Банка России № 3883-У	1	2	3	4	5
1	1	2	3	4	5
2	2	2	3	4	5
3	3	3	3	4	5
4	4	4	4	4	5

Группа качества ВПОДК

Буфер капитала по результатам надзорной оценки управления ОР и рисками ИБ

	Группа качества ВПОДК				
	1	2	3	4	5
Дополнительные требования к нормативам Н1.1, Н1.2, Н1.0 (Н20.1, Н20.2, Н20.0) **(буфер капитала)**	**0%**	**0%**	**1%**	**2%**	**3%**

Банк России
Центральный банк Российской Федерации

Приложения

Подходы к расчету величины необходимого капитала на покрытие ОР

Необходимый капитал на покрытие операционного риска в составе величины собственных средств (капитала) кредитной организации ($К_0$):

$$К_{необходимый,ОР} = \underbrace{К_{мин\_регуляторн,ОР}}_{№\ 346\text{-}П} + \underbrace{\Delta_{ИБ} + \Delta_{ОР}}_{№\ 3624\text{-}У}$$

где $К_{мин\_регуляторн,ОР}$ - минимальный капитал, выделяемый на покрытие операционного риска, необходимый для соблюдения минимального значения норматива достаточности капитала Н1.0

$\Delta_{ИБ}$ - **компонента необходимого капитала на покрытие совокупных убытков от реализации рисков ИБ**, определяемая в случае превышения контрольного показателя склонности к риску*) в части ИБ в течение года

$\Delta_{ОР}$ - **компонента необходимого капитала на покрытие совокупных убытков от реализации ОР без учета** $\Delta_{ИБ}$, определяемая в случае превышения контрольного показателя склонности к риску *) в части ОР (без учета ИБ) в течение года

*) контрольные показатели склонности к риску (риск аппетита) устанавливаются кредитной организацией самостоятельно и должны базироваться на внутренней оценке с учетом предыдущих надзорных оценок качестве системы ИБ и реализованных фактических потерь, покрываемых минимальным регуляторным капиталом на ОР, Если фактические потери за предыдущие года (год) превысили минимальный регуляторный капитал, то размер превышения включается в $\Delta_{ИБ}$ и $\Delta_{ОР}$ соответственно

Возможные меры, при выявлении нарушений требований Банка России

Федеральный закон от 10.07.2002 N 86-ФЗ (ред. от 31.12.2017) "О Центральном банке Российской Федерации (Банке России)"

- Статья 57.1. **Банк России устанавливает требования к системам управления рисками и капиталом**, внутреннего контроля кредитных организаций, в банковских группах, а также квалификационные требования к руководителю службы управления рисками, руководителю службы внутреннего аудита, руководителю службы внутреннего контроля кредитных организаций, головной кредитной организации банковской группы.
- Статья 57.2**. Банк России в порядке, установленном нормативным актом Банка России, проводит оценку качества систем управления рисками и капиталом**, внутреннего контроля кредитной организации, банковской группы, достаточности собственных средств (капитала) и ликвидности кредитной организации (банковской группы), их соответствия характеру и масштабу совершаемых кредитной организацией (в банковской группе) операций, уровню и сочетанию принимаемых рисков, включая определение объема и структуры операций как критериев такой оценки. **По результатам проведенной оценки в случае выявления несоответствия систем управления рисками и капиталом**, внутреннего контроля, достаточности собственных средств (капитала) и ликвидности кредитной организации (банковской группы) **установленным Банком России требованиям** и (или) характеру и масштабу совершаемых кредитной организацией (в банковской группе) операций, **уровню и сочетанию принимаемых рисков Банк России** в установленном им порядке **обязан направить в кредитную организацию (головную кредитную организацию банковской группы) предписание** о приведении систем управления рисками и капиталом, внутреннего контроля кредитной организации (банковской группы) в соответствие с требованиями Банка России, характером и масштабом совершаемых кредитной организацией (в банковской группе) операций, уровнем и сочетанием принимаемых рисков и (или) **об установлении для кредитной организации (банковской группы) индивидуальных предельных значений обязательных нормативов**.