Банк России

НОРМАТИВНЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ УПРАВЛЕНИЯ РИСКОМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.А. Бухтин

2020 г.

Операционная устойчивость

Базельский комитет по банковскому надзору работает над стандартом по операционной устойчивости для банков с 2018 года “Principles for operational resilience”, который планируется опубликовать в 2020 году

Операционная устойчивость – способность банка выполнять критичные операции банка в результате сбоев в работе.

Эта деятельность банка должна включать системную работу по выявлению угроз и потенциальных сбоев (в том числе связанную с **кибератаками**), защиту от них, обнаружение, реагирование и минимизацию воздействия сбоев в целях обеспечения выполнения критичных операций банка

Обеспечение операционной устойчивости потребует внутреннего взаимодействия следующих направлений деятельности банка:

управление операционным риском (ОР), включая риск информационной безопасности (киберриск)
(для этого Банк России выделяет в структуре управления операционным риском вопросы экономики от реализации риска ИБ (оценки потерь и капитала на их покрытие)

обеспечение информационной безопасности (ИБ)
(соблюдение стандартов и ГОСТ, технологического обеспечения ИБ)

обеспечение непрерывности деятельности, защиты критичных активов банка

управление аутсорсингом и контрагентами

Банк России планирует развивать требования к операционной устойчивости в рамках управления ОР

Базельский комитет по банковскому надзору относит риск ИБ (включая киберриск) к одному из самых важных видов операционного риска

В том числе, компания O.R.X, осуществляющая сбор информации о событиях ОР по всему миру, выделает риск ИБ как самый актуальный вид операционного риска в 2019 году, а также подчеркивает его значимость в будущем

ТОП операционных рисков в 2020 году

Актуальные виды рисков в 2020 году

1. **Риск ИБ (включая киберриск)**
2. Риск поведения (риск потерь клиентов из-за нарушения банком рыночных практик)
3. Технологический риск (риск информационных систем (ИС)
4. Регуляторный и комплаенс риск
5. Внутреннее и внешнее мошенничество

Виды рисков, влияние которых увеличится

1. Риски, вызванные макроэкономическими и геополитическими действиями
2. Риски, связанные с операционной устойчивостью
3. **Риск ИБ (включая киберриск)**
4. Риски изменений внутренней и внешней среды
5. Риск, связанный с действиями третьих лиц

* Operational Risk Horizon, O.R.X., 2020

Структура управления рисками ИБ и ОР

Структура требований Банка России к риску ИБ

Блок обеспечения ИБ банковского сектора (ДИБ)

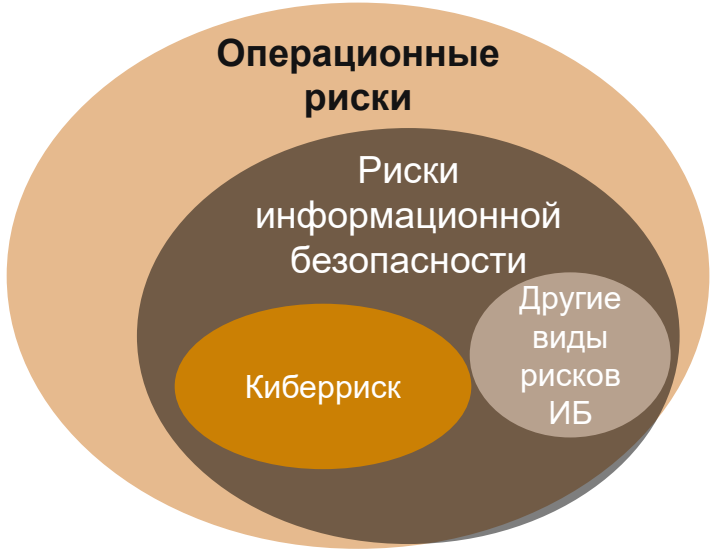
- Технические стандарты СТО БР
- ФинЦЕРТ
- «Стандарты финансовых (банковских) операций»
- Участие в проекте «Цифровая экономика»

Блок банковского надзора и регулирования

- Регулирование рисков ИБ в части экономики потерь
- Покрытия потерь капиталом и резервами
- Требования к управлению риском ИБ, Политике ИБ и СУОР (включая риск ИБ)
- Меры надзорного воздействия

Этапы издания нормативных актов по регулированию ОР, включая риск ИБ

Положение о СУОР	II квартал 2020 г.
Порядок ведения базы событий операционного риска (включая риск ИБ)	II квартал 2020 г.
Порядок расчета капитала по Базель III, с учетом статистики потерь	III квартал 2020 г.



Структура управления рисками ИБ и ОР в кредитной организации

Что сейчас

Служба ИБ

- Выявление инцидентов
- Контроль мер ИБ
- Мониторинг риска ИБ
- Технические стандарты
- Требования ГОСТ
- Меры по обеспечению ИБ
- …

Служба управления рисками

- Управление событиями ОР
- Покрытие потерь капиталом и резервами
- Анализ и определение потерь
- Оценка рисков
- Разработка мер по минимизации риска
- …

Издание Положения о СУОР, II квартал 2020 г.

Что должно быть в период с 2021-2022 гг.

Служба ИБ

- Выявление инцидентов
- Контроль мер ИБ
- Мониторинг риска ИБ
- Технические стандарты
- Требования ГОСТ
- Меры по обеспечению ИБ
- …

Информационный обмен

- Информирование об инцидентах ИБ
- Оценка потерь, организация мер по минимизации рисков

Служба управления рисками

- Управление событиями ОР
- Покрытие потерь капиталом и резервами
- Анализ и определение потерь
- Оценка рисков
- Разработка мер по минимизации риска
- …

Определение риска ИБ

Риск ИБ – риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения ИБ, в том числе применения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствия указанных процессов деятельности кредитной организации

Виды риска ИБ

Киберриск

- риск преднамеренных действий со стороны работников кредитной организации и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры (ОИИ) кредитной организации, в целях:
  - нарушения ОИИ и (или) прекращения их функционирования и (или) создания угрозы безопасности информации, подготавливаемой, обрабатываемой и хранимой ОИИ;
  - присвоения, хищения, изменения, удаления данных и иной информации (структуры данных, параметров и характеристик систем, программного кода) и режима доступа в результате несанкционированных действий, либо управленческих решений (злоупотребление полномочиями)

Другие виды

- виды риска ИБ, связанные с обработкой (хранением, уничтожением) информации без использования ОИИ

Риск ИБ имеет дополнительные элементы классификации

Проект положения Банка России «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (проект положения) *

Основные требования проекта Положения, которые вводятся во II квартале 2020 года:

Требования к системе управления ОР

Требования к управлению риском ИБ

Требования к управлению риском ИС

Требования к ведению базы событий ОР

прямые потери от риска ИБ (киберриска)

прямые потери от других видов ОР, например, связанных:
Со сбоями ИС,
с ошибками процессов

Для оценки величины необходимого капитала на покрытие потерь от риска

Проектом положения предусмотрена дифференциация требований и сроков внедрения системы управления ОР в зависимости от вида кредитной организации и типа лицензии

* Планируется к утверждению во II квартале 2020 г.

Кредитная организация в целях управления риском ИБ обеспечивает функционирование системы ИБ, в том числе:

- определяет политику ИБ
- выявляет и идентифицирует риск ИБ и события риска ИБ
- обеспечивает защиту от угроз безопасности информации
- осуществляет реагирование на выявленные события риска ИБ и восстановление деятельности кредитной организации в случае реализации таких событий
- осуществляет обмен информацией о событиях риска ИБ
- ежегодно тестирует на проникновение и анализ уязвимостей ИБ объектов информационной инфраструктуры
- планирует, реализует, контролирует и совершенствует комплекс мероприятий, направленных на повышение эффективности управления риском ИБ и уменьшение негативного влияния риска ИБ
- устанавливает и реализует программы контроля
- проводит независимую оценку соответствия уровня защиты информации в отношении объектов информационной инфраструктуры кредитной организации
- обеспечивает соответствие фактических значений контрольных показателей уровня риска ИБ принятым в кредитной организации значениям

и др.

Структура информационного обмена

Несанкционированный доступ

Утечка информации

Кибератаки

Потеря информации

Вредоносное ПО

Антивирусы

IPS (межсетевые экраны)

IDM (управление учетными записями)

PUM (контроль привилегированных users)

Защита от **DDoS**

WAF (защита веб-приложений)

Анализ исходного кода

Antifraud

Защита от таргетированных атак

SIEM

UEBA (мониторинг действий users)

DLP (утечка данных)

Шифрование

Система отказоустойчивости

Обеспечение ИБ

Кредитная организация

База инцидентов ИБ, вкл. поступившие, предотвращенные и пропущенные инциденты ИБ с прямыми и непрямыми потерями

Передача информации об инцидентах ИБ с прямыми потерями на ежемесячной основе

База событий операционного риска

Передача информации об инцидентах ИБ

ФинЦЕРТ

Оперативные мероприятия

Расчет величины необходимого капитала на покрытие потерь от риска

Функции подразделения информационной безопасности

Функции по обеспечению ИБ 1-й уровень защиты (оперативный)

- разработка политики ИБ
- контроль соблюдения работниками кредитной организации мероприятий обеспечения ИБ и защиты информации и выполнение других задач
- осуществление планирования и контроля процессов обеспечения ИБ в рамках комплекса мероприятий, направленных на повышение эффективности управления риском ИБ и уменьшение негативного влияния риска ИБ
- разработка предложений по совершенствованию процессов обеспечения ИБ
- составление отчетов по обеспечению ИБ и направление их лицу, ответственному за обеспечение ИБ
- соблюдение национальных стандартов Российской Федерации:

ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности»

ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»

ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»

ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»

Функции по управлению риском ИБ 2-й уровень защиты (управление риском ИБ)

- соблюдение процедур управления ОР (выявление, сбор, регистрация событий риска ИБ в базе событий, мониторинг риска ИБ)
- ведение базы событий риска ИБ и потерь от их реализации
- участие в реализации комплекса мероприятий, направленных на повышение эффективности управления риском ИБ
- мониторинг эффективности управления риском ИБ
- составление отчетов по рискам ИБ и направление их в службу управления рисками и лицу, ответственному за обеспечение ИБ, коллегиальному исполнительному органу кредитной организации
- мониторинг соблюдения сигнальных и контрольных значений контрольных показателей уровня риска ИБ
- участие в разработке внутренних документов по управлению риском ИБ
- информирование работников кредитной организации по вопросам, связанным с управлением риском ИБ

и др.

Политика ИБ кредитной организации

Политика ИБ кредитной организации определяет:

- функции и ответственность коллегиального исполнительного органа и работников кредитной организации (головной кредитной организации банковской группы) в рамках управления риском ИБ
- основные принципы и подходы к обеспечению функционирования системы обеспечения ИБ
- порядок взаимодействия подразделений кредитной организации по выполнению функций информационной безопасности (вкл. распределение ролей и задач)
- сигнальные и контрольные значения контрольных показателей уровня риска ИБ
- основные принципы и подходы к организации контроля за функционированием системы обеспечения ИБ
- требования к организации ресурсного (кадрового и финансового) обеспечения системы обеспечения ИБ
- требования к внешним контрагентам, выполняющим функции обеспечения ИБ (аутсорсинг), а также определение порядка взаимодействия и ответственности между ними

Политику ИБ утверждает коллегиальный исполнительный орган кредитной организации, который несет ответственность в целом за соблюдение требований политики ИБ

В последующем в рамках надзорных проверок будет осуществляться проверка и оценка качества составления политики ИБ кредитной организации и ее соблюдения (банковский надзор).
При несоблюдении требований к политике ИБ будут применяться меры надзорного воздействия

Порядок взаимодействия подразделения ИБ с другими участниками системы управления ОР

Подразделение ИБ	• Выявление, регистрация и учет инцидентов ИБ (события риска ИБ), определение элементов классификации и источников угроз, уязвимостей, успешности реализации угрозы (компьютерной атаки) • Определение банковских процессов, подверженных реализации риска ИБ, информационных систем, фактов компрометации объектов информационной инфраструктуры • Немедленное реагирование на выявленные инциденты ИБ (события риска ИБ) в соответствии с установленным в КО порядком (например, блокировка портов, прав доступов)	• Передача информации об инциденте в службу управления рисками • Определение эффективности мер по обеспечению ИБ и мер немедленного реагирования по результатам реализованного инцидента ИБ (события риска ИБ) • Принятие участия в восстановлении деятельности КО
Служба управления рисками	• Определение масштаба и степени влияния инцидента (события риска ИБ) на другие риски и банковские процессы • Классификация инцидента ИБ (события риска ИБ) по методологии ОР и отражение его в базе событий	• Определение совместно с Владельцами рисков/процессов потерь от инцидента ИБ (события риска ИБ) • Определение эффективности мер минимизации других рисков, зависимых от реализованного инцидента ИБ (события риска ИБ)
Подразделения банка	• Реагирование на выявленные инциденты ИБ (события риска ИБ) со стороны бизнес-подразделений, сопровождающих и обеспечивающих подразделений (блокировка счетов, приостановление операций, взаимодействие с клиентами и третьими лицами и т.п.)	• Определение последствий от инцидента ИБ (события риска ИБ) и предоставление информации в службу управления рисками о наличии и размере потерь КО и его клиентов/контрагентов
Уполномоченный коллегиальный орган	• Рассмотрение результатов процедуры мониторинга ОР, включая риск ИБ, в составе ежеквартального и годового отчета об управлении ОР • Рассмотрение отчетов о результатах оценки эффективности выполнения процедур управления ОР (в том числе на предмет их полноты и корректности)	• Дает поручения по разработке мероприятий, направленных на повышение качества системы управления ОР и уменьшение негативного влияния ОР, с указанием ответственных за реализацию мероприятий подразделений и сроков выполнения

реализация мероприятий, направленных на повышение качества системы управления ОР и уменьшение негативного влияния ОР

Проект положения Банка России «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (проект положения)

- первый нормативный акт, выпускаемый в целях внедрения нового стандартизированного подхода к оценке операционного риска (ОР) для целей расчета норматива достаточности капитала Базель III
- разработан в 2019 году, два раза выносился на публичное обсуждение с банковским сообществом и находится на согласовании в Банке России

Задачи проекта Положения:

1. Формализация единых требований к качеству системы управления ОР, включая унификацию требований к отдельным видам ОР, управляемыми отдельными специализированными подразделениями, в том числе риском информационной безопасности (ИБ)

2. Подготовка баз данных банков для использования данных в расчете капитала по стандартизированному подходу к оценке ОР (включая киберриск)

3. Установление требований к оценке и выделению необходимого капитала на покрытие потерь от киберрисков. Адекватная оценка возможных потерь от ОР для целей выделения на них фондов покрытия потерь, как в бюджете доходов и расходов, так и определение части экономического капитала на их покрытие.

Подход к оценке объема капитала, необходимого для покрытия потерь от реализации событий ОР в рамках ВПОДК *

Объем капитала, необходимого для покрытия потерь от реализации событий операционного риска:

$$К_{необ\_К_i,ОР} = \underbrace{К_{мин\_К_i,ОР}}_{\text{по № 652-П}} + \Delta_{К_i,ИБ} + \Delta_{К_i,ОР},$$

где:

- $К_{необ\_К_i,ОР}$ - минимальный регуляторный капитал на покрытие потерь от реализации событий ОР, включаемый в состав совокупного объема необходимого капитала, соответствующего $К_i$ в соответствии с требованиями Указания Банка России № 3624-У и выделяемый на покрытие потерь от реализации событий ОР, необходимый для соблюдения минимально допустимого числового значения норматива достаточности капитала Н1.i
- $\Delta_{К_i,ИБ}$ - компонент объема капитала, необходимого для покрытия потерь от реализации событий ОР, соответствующего $К_i$ в соответствии с методикой, предусмотренной Положением Банка России № 646-П, соответственно на покрытие прямых потерь для $\Delta_{К_1,ИБ}$ и $\Delta_{К_2,ИБ}$ прямых потерь (для $\Delta_{К_0,ИБ}$ – совокупных (прямых и косвенных) потерь) от реализации событий риска ИБ
- $\Delta_{К_i,ОР}$ - компонент объема капитала, необходимого для покрытия потерь от реализации событий ОР, соответствующего Кi в соответствии с методикой, предусмотренной Положением Банка России № 646-П, соответственно на покрытие для $\Delta_{К_1,ОР}$ и $\Delta_{К_2,ОР}$ прямых потерь (для $\Delta_{К_0,ОР}$ – совокупных (прямых и косвенных) потерь) от реализации ОР за вычетом потерь от событий риска ИБ

* Определено в приложении 2 к проекту положения

Банк России

СПАСИБО
ЗА ВНИМАНИЕ