COMPLIANCE CONTROL

Готовимся к «стандартному» будущему: выстраиваем внутренние процессы в соответствии с ГОСТ Р 57580.3 и ГОСТ Р 57580.4

Павел Лего
Руководитель направления российского консалтинга и аудита

Структура ГОСТ 57580.X

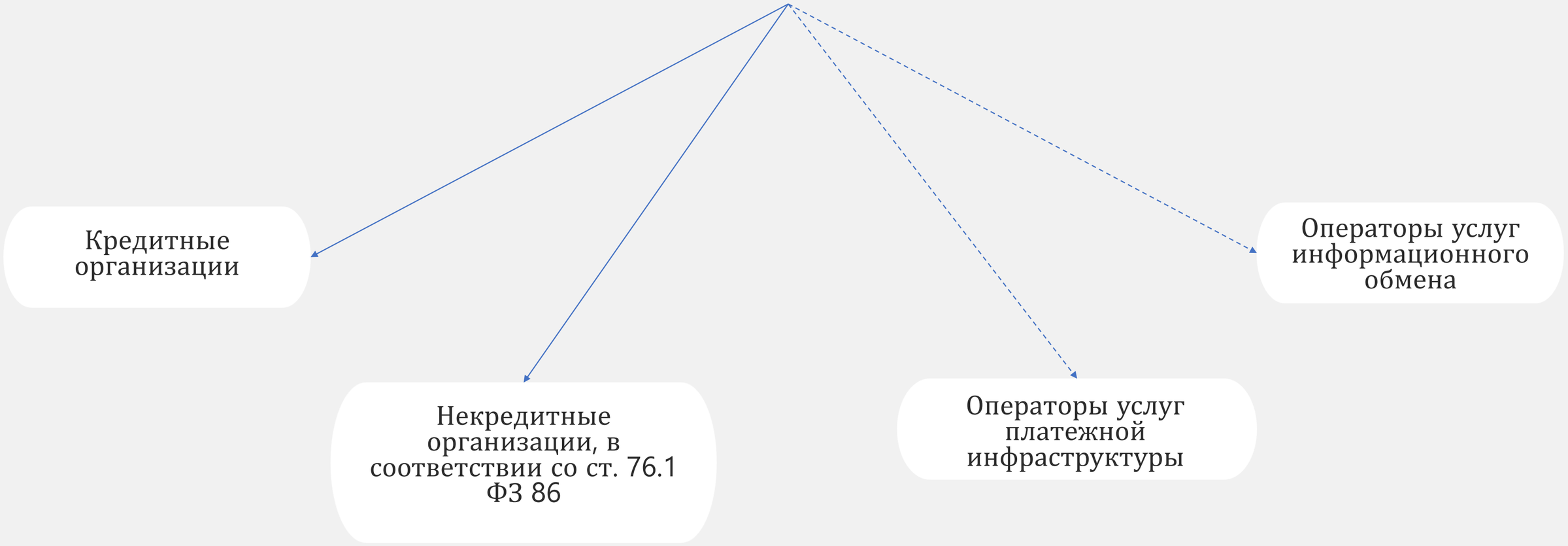
Комплекс национальных стандартов «Безопасность финансовых (банковских) операций»

Семейство стандартов УР	Управление риском реализации информационных угроз и обеспечение операционной надежности (ГОСТ 57580.3 - 2022)
	Методика оценки зрелости (?)
Семейство стандартов ОН	Обеспечение операционной надежности (ГОСТ 57580.4 – 2022)
	Методика оценки соответствия (?)
Семейство стандартов ЗИ	Защита информации финансовых организаций (ГОСТ 57580.1 - 2017)
	Методика оценки соответствия (ГОСТ 57580.2 - 2018)

Применимость ГОСТ Р 57580.3 – 2022 и ГОСТ Р 57580.4-2022

ГОСТ Р 57580.3-2022

ГОСТ Р 57580.3-2022



Выстраивание процессов

Планирование

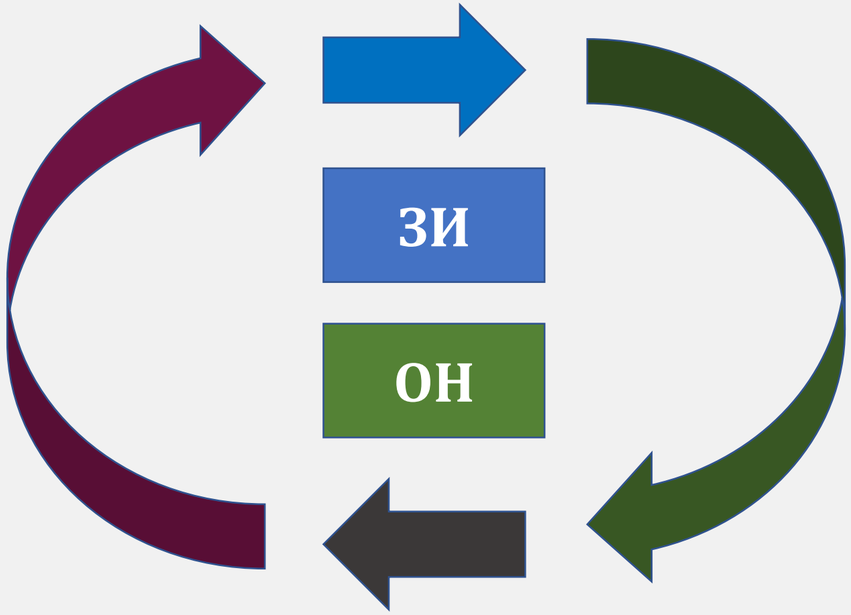
Принятые значения КПУР

Реализация

Контроль

Фактические значения КПУР

Совершенствование



Выстраивание процессов

Планирование

- Ресурсное и кадровое обеспечение, организация обучения
- Определение сигнальных и контрольных значений по управлению рисками
- Определение ключевых показателей в рамках операционной надёжности
- Выявление, идентификация и оценка риска (база событий риска)
- Политика управления риском реализации информационных угроз
- Порядок и методы обеспечения операционной надёжности

Определение ключевых показателей в рамках управления рисками

Определение и установление КИР (Ключевой индикатор риска).

Определение и установление КПУР (Контрольный показатель уровня риска).

Определение и установление сигнального значения КПУР.

Определение и установление контрольного значения КПУР.

Определение способов возмещения запланированных (ожидаемых) и незапланированных потерь

Определение ключевых показателей в рамках обеспечения операционной надежности

Целевая точка восстановления данных (ЦТВД).
Состояние (объем), до которого необходимо восстановить данные, используемые в рамках предоставления финансовых и (или) информационных услуг, для обеспечения возобновления их выполнения.

Целевое время восстановления.
Период времени, установленный для возобновления предоставления финансовых и (или) информационных услуг после инцидента, связанного с реализацией информационных угроз.

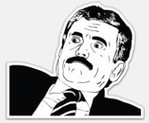
Допустимое время простоя и (или) деградации бизнес- и технологических процессов.
Допустимый временной период, в течение которого происходит простой и (или) деградация бизнес- и технологических процессов.

Допустимая доля деградации бизнес- и технологического процесса.
Допустимое отношение общего количества финансовых (банковских) операций, совершенных во время деградации в рамках инцидента к ожидаемому количеству операций за тот же период в случае непрерывного оказания услуг.

Организационная структура (определение зон ответственности)

Ресурсное и кадровое обеспечение службы ИБ и службы управления рисками:

- Оценка необходимого ресурсного (кадрового и финансового) обеспечения для определения состава основных ресурсов.
- Определение и обеспечение необходимой численности и требуемой компетенции работников при организации ресурсного (кадрового и финансового) обеспечения служб ИБ. Повышение квалификации.



Определение ответственного за функционирование системы управления риском и назначение его куратором службы ИБ.

Участие совета директоров (наблюдательного совета) и коллегиального исполнительного органа финансовой организации в решении вопросов управления риском.

Организация целевого обучения работников, задействованных в рамках управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации

Построение трёх линий защиты в системе управления рисками

Центры компетенций (Информирование о выявленном риске, оценку выявленных рисков, разработку и внедрение мероприятий, направленных на уменьшение влияния риска, и мониторинг уровня риска в своих процессах).

Службы управления рисками и служба информационной безопасности.

Уполномоченное подразделение (Независимое от службы ИБ и службы управления рисками, уполномоченное проводить оценку эффективности функционирования системы управления риском, подготовку методологии, данных и внутренней отчетности в рамках управления риском).

Выстраивание процессов

Реализация

- Защита информации финансовой организации
- Обеспечение операционной надежности
- Выявление событий риска
- Реагирование на инциденты в отношении критичной архитектуры и анализ причин
- Восстановление функционирования бизнес- и технологических процессов
- Обеспечение осведомленности об актуальных угрозах

Разработка (доработка) комплектов документов (Обеспечение операционной надежности)

- Положение по обеспечению операционной надежности.
- Управление критичной архитектурой на всех стадиях жизненного цикла.
- Журнал (реестр) учета элементов критичной архитектуры.
- Реестр бизнес-процессов.
- Реестр информационных систем.
- Моделирование информационных угроз.

Разработка (доработка) комплектов документов (Управление рисками ИБ)

- Внесение изменений в Политику ИБ:
  - кадровое и ресурсное обеспечение;
  - функции и ответственность коллегиального исполнительного органа;
  - сигнальные и контрольные значения;
  - требования к третьим лицам;
  - принципы обеспечения ИБ и управления риском.
- Политика управления рисками ИБ.
- Порядок ведения базы событий риска.

Порядок реагирования на риск реализации информационных угроз

- Уклонение от риска, предусматривающее отказ от выполнения отдельных бизнес-процессов в связи с высоким уровнем риска
- Передача риска, предусматривающая страхование, передача риска причастной стороне
- Принятие риска, в рамках сигнальных и контрольных значений КПУР, а также на основе финансового покрытия потерь от реализации риск
- Разработка и реализация мероприятий, направленных на уменьшение негативного влияния риска

Механизмы обеспечения операционной надежности

- **Проведение сценарного анализа,** проведение анализа влияния на бизнес с учетом результатов сценарного анализа.
- **Управление стандартами конфигурирования** .
- **Обеспечение** необходимой и достаточной производительности объектов информатизации.
- **Применение отказоустойчивых решений.**
- **Управление уязвимостями** в критичной архитектуре.
- **Обеспечение безопасности при удаленном техническом обслуживании**
- **Выбор поставщиков услуг**

Процесс обучения

- **Обучение, (переподготовка)** работников ИБ.
- **Регулярное прохождение дополнительного обучения,** переподготовки (повышения квалификации) в области ИБ.
- **Повышение осведомленности (инструктаж) работников** в области защиты информации.
- **Целевое обучение работников,** в рамках управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации.
- **Планы по обучению и повышению** осведомленности работников в части противостояния реализации информационных угроз.

Выстраивание процессов

Контроль

Проведение самооценки процессов зрелости

Мониторинг риска реализации угроз

Проведение независимой оценки процессов зрелости

Проведение сценарного анализа и тестирования

Оценка эффективности функционирования системы управления риском

Организация внутренней отчетности, в том числе результаты обучения

Организация контрольных мероприятий и постоянного мониторинга

- **Проведение самооценки** (минимальный уровень) и **независимой оценки** (стандартный и усиленный) зрелости процессов обеспечения операционной надежности и защиты информации.
- **Проведение сценарного анализа** и тестирования в отношении критичной архитектуры **(киберучения).**
- **Оценка эффективности функционирования системы управления риском (мониторинг риска реализации информационных угроз).**
- **Периодический контроль (тестирование)** полноты реализации технических мер обеспечения операционной надежности.
- **Проведение проверок знаний** работников финансовой организации.

Организация внутренней отчетности

- **Фиксация результатов проведения самооценок и аудитов ОН и ЗИ** в виде отчетов, содержащих мотивированное суждение об уровне зрелости процессов совершенствования систем управления.

- **Доведение результатов самооценок и аудитов ОН и ЗИ** до совета директоров (наблюдательного совета) и исполнительного органа финансовой организации, а также должностного лица, ответственного за функционирование системы управления риском.

- **Организация и выполнение деятельности по хранению, предоставлению санкционированного доступа и использованию материалов** (в частности, отчетов), получаемых в процессе проведения самооценок и аудитов ОН и ЗИ.

- **Включение в отчетность сведений** о ведении претензионной работы в отношении ее причастных сторон, в том числе клиентов.

- **Ведение отчетности о результатах мониторинга риска.**

Проведение сценарного анализа и тестирования

- **Установление и реализация программ по сценарному анализу** и тестированию готовности противостоять реализации информационных угроз.
- **Определение во внутренних документах** методологии и порядка проведения сценарного анализа и тестирования.
- **Разработка сценариев** и проведение периодических тестирований готовности противостоять реализации угроз в условиях, приближенных к реальным.
- **Оценка подготовленности работников** противостоять реализации информационных угроз, в том числе компьютерных атак.
- **Оценку достаточности ресурсного (кадрового и материального)** обеспечения для реагирования на инциденты и восстановления после их реализации.

Выстраивание процессов

Совершенствование

Обеспечение соответствия фактических значений КПУР принятым

Выявление необходимости пересмотра применяемых мер обеспечения операционной надежности

Совершенствование системы управления рисками и ОН

- **Проведение анализа необходимости совершенствования системы** управления риском реализации информационных угроз.
- **Принятие решений по совершенствованию системы** управления риском реализации информационных угроз.
- **Проведение и фиксация результатов (свидетельств) анализа** необходимости совершенствования процесса системы обеспечения операционной надежности (изменения принципов ОН, инцидентов и недостатков, пересмотр технических мер).
- **Организация и выполнение деятельности по совершенствованию** применяемых организационных и технических мер (анализ причин и последствий реализации инцидентов, рамках консультаций с экспертами внутри финансовой организации).

Вопросы?

p.lego@compliance-control.ru

COMPLIANCE CONTROL

info@compliance-control.ru

+7 499 136-27-66

compliance-control.ru