RTM GROUP

Операционная надёжность и риски: важнейшие нормы в рамках одного вебинара

RTM GROUP

Объединяем IT,
право и безопасность

Далее

Спикеры

Дмитрий Кобец

- **Заместитель директора** технического Департамента;
- **Эксперт** в сфере информационной безопасности;
- **Профессиональный опыт** в сфере информационных технологий и информационной безопасности с 2009 года.

Кирилл Чекудаев

- **Ведущий эксперт** по управлению рисками;
- **Кандидат** экономических наук;
- **Стаж профессиональной деятельности** по экономическим направлениям с 2003 года.

О компании RTM Group

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Информационная безопасность:

Аудиты, пентест, КИИ, защита ПДн, оценка защищённости и др.

Компьютерно-технические экспертизы:

44-ФЗ, расследования инцидентов, ИТ-контракты и др.

ИТ-право:

Судебное и досудебное урегулирование, сопровождение и др.

СОДЕРЖАНИЕ

О Положениях 787-П и 779-П

Обеспечение операционной надежности

Критически важные процессы БКО 787-П

- Выполнение **кассовых** операций;
- **Онлайн-сервисы** дистанционного обслуживания;
- Работа с **биометрическими** персональными данными.
- Выполнение операций на **финансовых рынках** (24 часа пороговый уровень)**;**
- Открытие и ведение **банковских счетов;**
- **Размещение** привлеченных во вклады денежных средств;
- **Осуществление** переводов денежных средств;
- **Привлечение** денежных средств во вклады;

Пороговый уровень времени простоя или деградации: 2-6 часов

Целевые показатели операционной надежности

Целевой показатель	Определение
Допустимая доля деградации технологического процесса	Общее количество операций в период инцидентов/ общее количество операций непрерывного функционирования
Допустимое время простоя и (или) деградации технологических процессов кредитных организаций в рамках инцидента операционной надежности	Не превышающий значения установленное Приложением 1
Допустимое суммарное время простоя и (или) деградации технологического процесса кредитной организации	Общее допустимое время простоя в случае превышения допустимой доли деградации технологического процесса в течение очередного календарного года
Показателя соблюдения режима работы (функционирования) технологического процесса	Время начала, время окончания, продолжительности и последовательности процедур в рамках технологического процесса

Фиксация превышения допустимой доли деградации технологических процессов

- **Фактическое время простоя** и (или) деградации технологического процесса, исчисляемого по каждому инциденту операционной надежности;
- **Фактическая доля деградации** технологического процесса в рамках отдельного инцидента операционной надежности;
- **Суммарное время** простоя и (или) деградации технологического процесса за последние двенадцать календарных месяцев.

Объекты информационной инфраструктуры

Критическая архитектура

- Технологические процессы
- Подразделения, ответственных за разработку, поддержание выполнения, реализацию технологических процессов
- Объекты информационной инфраструктуры
- Технологические участки технологических процессов
- Поставщики услуг
- Субъекты доступа
- Взаимосвязи и взаимозависимости с участниками технологических процессов
- Каналы передачи защищаемой информации, в соответствии с 683П/757П

Требования к управлению изменениями критичной архитектуры

Управление уязвимостями КА

Управление уязвимостями и обновлениями (исправлениями) объектов

Планирование и внедрение изменений КА

Управление конфигурациями (настраиваемыми параметрами) объектов

Что делать в случае возникновения инцидента?

1. Выявление и регистрация инцидентов
2. Реагирование на инциденты
3. Восстановление функционирования
4. Проведение анализа причин и последствий
5. Организация взаимодействия между подразделениями, Банком России, другими участника

Взаимодействие с поставщиками в сфере ИТ

Нейтрализация (787П)/управление рисками реализации (779П)

Привлечение поставщиков услуг, в том числе защиту своих объектов ИИ от возможной реализации информационных угроз со стороны поставщиков услуг

Технологическая зависимость функционирования объектов информационной инфраструктуры от поставщиков услуг в сфере информационных технологий

Меры

- **Сценарный** анализ;
- **Тестирование**;
- **Организационные** и технические меры в отношении субъектов доступа (внутренних нарушителей);
- **Обмен и использование** информации об актуальных сценариях реализации информационных угроз;
- **Обеспечение защиты** дистанционной работы сотрудников;
- **Выполнение требований**, направленные на противодействие целевым компьютерным атакам (для субъектов критической информационно инфраструктурой);

Что должно быть отражено в документах

- **Определение** и описание состава процедур
- **Определение перечня** и порядка организационного взаимодействия подразделений (организационная структура)
- **Определение порядка** осуществления контроля за соблюдением требований к операционной надежности в рамках системы внутреннего контроля (для НФО установление функций контроля подразделениям)
- **Выделение ресурсного обеспечения** для выполнения требований к операционной надежности;
- **Порядок утверждения** и условия пересмотра процедур.

Должны!

- **Моделировать информационные угрозы** в отношении критичной архитектуры;
- **Планировать применение организационных** и технических мер, направленных на реализацию требований к операционной надежности;
- **Обеспечивать реализацию требований** к операционной надежности на стадиях создания, ввода в эксплуатацию, эксплуатации, модернизации, вывода из эксплуатации объектов информационной инфраструктуры;
- **Обеспечивать контроль соблюдения** требований к операционной надежности (НФО в отношении элементов критической инфраструктуры).

Регистрация

- **Данных,** используемых для фиксации превышения установленных значений целевых показателей операционной надежности;
- **Данных,** позволяющих выявить причину превышения установленных значений целевых показателей операционной надежности;
- **Результата реагирования** на инцидент операционной надежности (о принятых мерах и проведенных мероприятиях по реагированию на выявленный кредитной организацией или Банком России инцидент операционной надежности).
- **Кредитные организации** фиксируют в базе событий операционных рисков!

Информирование Банка России

- **О выявленных событиях** операционного риска, связанных с нарушением операционной надежности, а также о принятых мерах и проведенных мероприятиях по реагированию на указанные события операционного риска, связанные с нарушением (инцидент) операционной надежности, организацией или Банком России;
- **О планируемых публичных мероприятиях,** в отношении событий операционного риска, связанных с нарушением операционной надежности

Изменения в 716-П

Указания 6103-У от 25.03.2022 «О внесении изменений в Положение Банка России от 8 апреля 2020 года № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Вступает в силу 01.10.2022

Взаимосвязь

- 161ФЗ
- 683П
- 719П (вместо 382П)
- 744П
- ГОСТ 57580.1-2017
- ГОСТ 57580.2-2018

Вступает в силу 01.01.2023

(Изменения в Приложении 1 Контрольные показатели уровня операционного риска)

Общие изменения 716П

Основные дополнения:

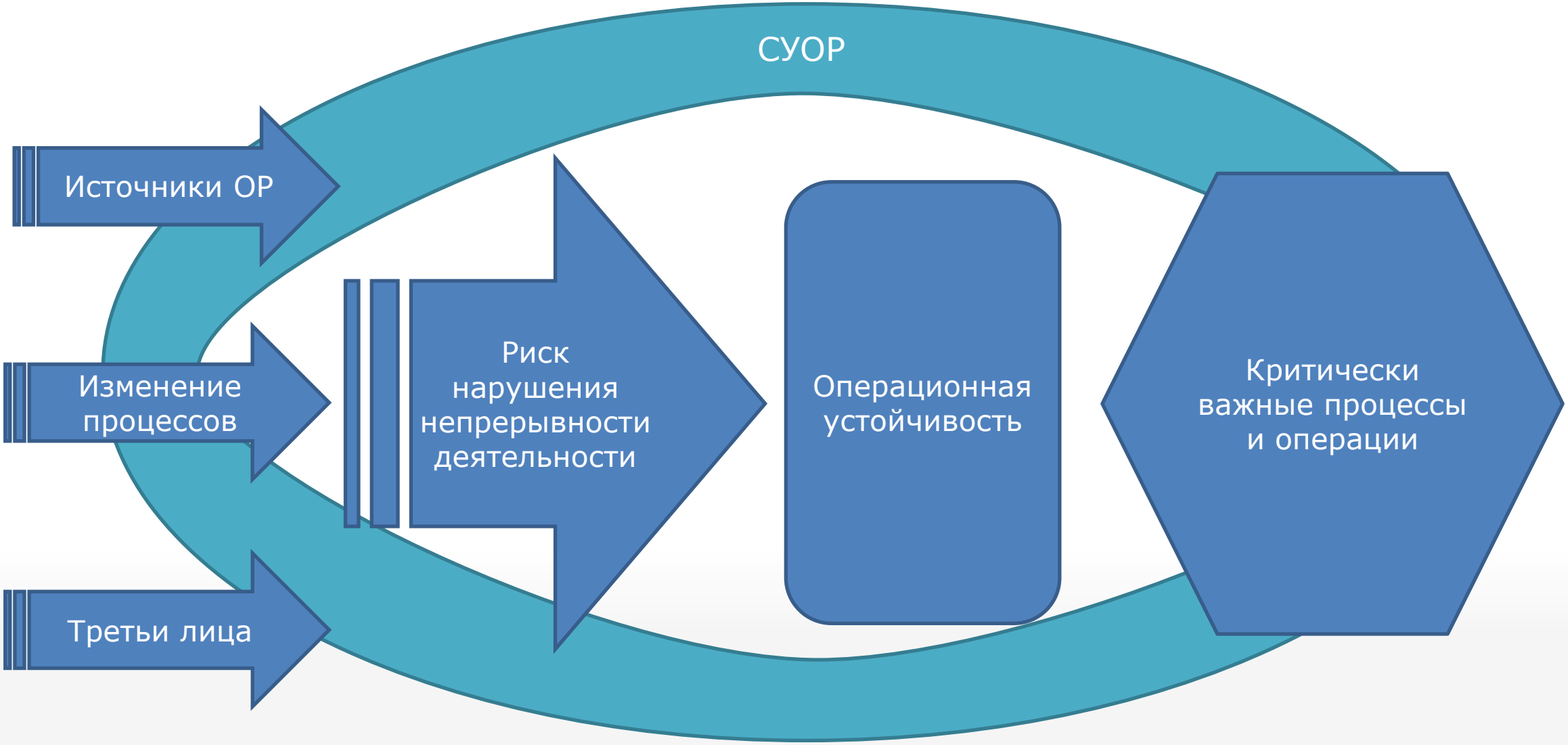
- Риск нарушения непрерывности деятельности;
- Операционная надежность и устойчивость;
- Технологические процессы;
- Описание информационной архитектуры;
- Моделирования угроз;
- Изменения в критически важные процессы;
- Требования к информационным системам третьих лиц;
- Разграничение полномочий подразделений; ответственных за обеспечение ИБ и ИС;
- Предоставление отчетов о результатах оценки;
- Изменение уровня контрольных и сигнальных значений;
- Оценка эффективности процессами; предотвращения неподтверждённых переводов средств клиентов-физических лиц;
- Качественные и контрольные показателей.

Убрано:

- Обеспечивающие процессы;
- Специализированные отчеты по 382П.

Рискоориентированный подход

Операционная устойчивость



Изменение требований к ИБ

Добавили:

- Мониторинг риска информационной безопасности;
- Обеспечение осведомленности кредитной организации и участников технологических процессов об актуальных угрозах безопасности информации;
- Подчинение лицу, осуществляющие функции единоличного исполнительного органа (не заместителю);
- Противодействие внутренним нарушителям;
- Требования по количественным контрольным показателя информационной безопасности, связанные с переводом денежных средств без согласия клиента (161ФЗ);
- Учет оценки уровня защиты информации процессов 1 и 5 ГОСТ 57580.1-2017;
- Оценка выполнения к защите информации 683П, 719П, 747П по методике ГОСТ 57580.2-2018.

С 01.01. 2023

Убрали:

- Оценка эффективности управления риском информационной безопасности;
- Специализированные отчеты по 382П;
- Ответственность за риски ИС.

Изменение требований к ИС

Добавили:

- Перечень информационных систем;
- Описания архитектуры и состав элементов ИС;
- Структура информационного обмена между элементами: подразделениями, работниками и третьими лицами;
- Элементы и структуру информационного обмена третьих лиц;
- Требования к договорам с третьими лицами.

Убрали:

- Ответственность за риски ИБ.

Итоги

- **Управление операционной надежностью** возможно реализовать, и мы можем в этом помочь.
  - **систематизировать** управление операционной надежностью с включением в неё процессов управления рисками ИБ и ИС с нуля;
  - **надстроить** процессы управления операционной надежностью над существующей системой управления операционным риском.
- **При реализации** системы управления операционной надежностью недостаточно разработать документы, необходимо планирование процессов и их последующая реализация.

ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ!

Дмитрий Кобец

Эксперт в сфере информационной безопасности

Заместитель директора технического департамента **RTM Group**

Кирилл Чекудаев

Эксперт в сфере управления рисками

Ведущий эксперт **RTM Group** по управлению рисками


+7 (495) 197-64-95


info@rtmtech.ru


https://rtmtech.ru


rtm.group


t.me/kurilka_ib