RTM GROUP

Разбор 7 и 8 главы 716-П: Основные моменты и особенности

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.

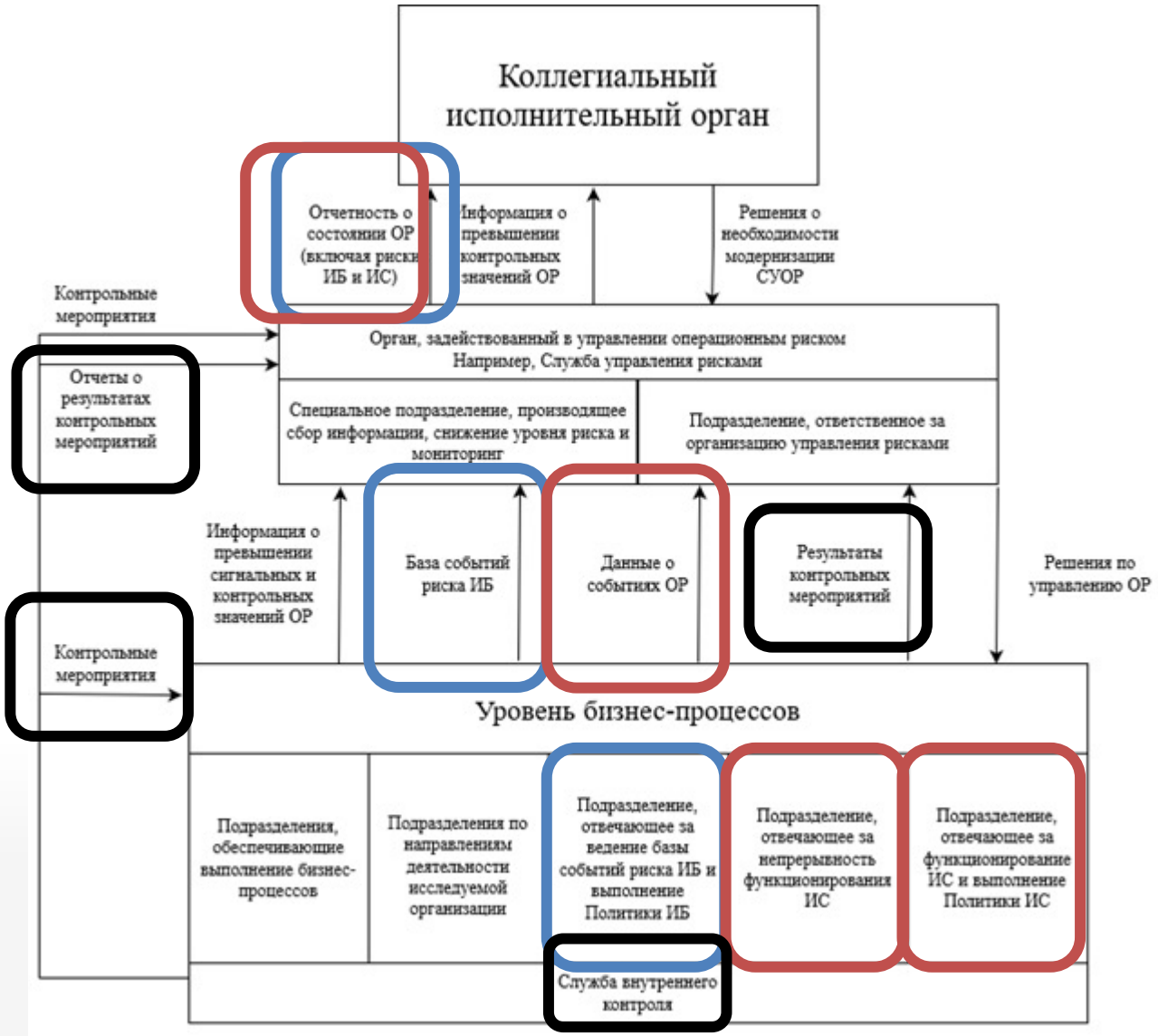
Компьютерно-технические экспертизы:
44-ФЗ, расследования инцидентов, ИТ-контракты и др.

ИТ-право:
Судебное и досудебное урегулирование, сопровождение и др.

СОДЕРЖАНИЕ

Место рисков ИБ и ИТ в СУОР

- элементы управления риском ИБ;
- элементы управления риском ИС;
- элементы контроля;



Особенности управления рисками ИБ

- Нужен **отдельный** комплект документов.
- **Отдельная отчетность** руководству.
- **Может** вестись отдельная база событий риска (но не должна)
- Минимальная классификация рисков ИБ:
  - риски обработки информации **с использованием** ИС (киберриск);
  - риски обработки информации **без использования** ИС.
- Вывод ИС из строя не по причине инцидента – **не событие** риска ИБ (хотя налицо нарушение доступности).

Примерный комплект документации (риски ИБ)

Наименование документа	Описание / содержание
Политика ИБ	Контрольные и сигнальные значения рисков ИБ Порядок контроля и отчетности Формы отчетных документов
Положение о Службе ИБ	Распределение функций и обязанностей по управлению риском ИБ Порядок управления риском ИБ силами Службы
База событий риска ИБ	Данные о произошедших инцидентах ИБ и результатах их обработки
Технологическое описание системы управления риском (СУР) ИБ	Порядок управления риском ИБ Элементы СУР и её обеспечение
Порядок управления риском ИБ	Процедуры управления риском ИБ

Особенности управления рисками ИС

- Нужен **отдельный** комплект документов.
- **Отдельная отчетность** руководству.
- Риск ИС = риск отказов и/или нарушения функционирования применяемых ИС **не вследствие инцидентов ИБ.**
  - Внешняя DDoS-атака – событие **риска ИБ**.
  - Отключение электричества – событие **риска ИС**.
- Нужно дорабатывать план **ОНиВД**, если такой есть.

Обеспечение функционирования ИС

- Назначить ответственных лиц.
- Разработать требования к ИС.
  - К структуре;
  - К надежности;
  - К жизненному циклу;
  - К качеству данных.

Обеспечение непрерывности функционирования ИС – что делать?

- **Назначить** ответственных лиц.
- **Классифицировать** ИС по критичности остановки их работы.
- **Настроить** процессы резервного копирования критичных активов.
- **Проводить** периодический контроль соблюдения требований.

Управление качеством данных

- Определить требования к обеспечению качества данных, включая **требования к данным**.
  - Актуальность, точность и т.д.
- Разработать **методику** обеспечения качества данных.
  - Как оценивать, как контролировать, как повышать – методы и критерии.
- Разработать **порядок** обеспечения качества данных.
  - Предложить конкретные процедуры.

Точность

Структура

Полнота

Уникальность

Своевременность

Аутентичность

Примерный комплект документации (риски ИС)

Наименование документа	Описание / содержание
Политика ИС	Классификация ИС Требования к ИС Порядок контроля и отчетности Порядок управления риском ИС
Положение о Департаменте ИТ	Распределение функций и обязанностей по управлению риском ИС Порядок управления риском ИС силами Департамента
Должностная инструкция лица, ответственного за функционирование ИС	Функции, обязанности, полномочия Требования к квалификации и место в иерархии
Должностная инструкция лица, ответственного за непрерывность работы ИС	Функции, обязанности, полномочия Требования к квалификации и место в иерархии
Методика обеспечения качества данных	Методы и критерии оценки и контроля качества данных
Порядок обеспечения качества данных	Процедуры управления качеством данных

Итоги

- **Систему управления** рисками ИБ и ИС можно реализовать по-разному, и мы можем в этом помочь.
  - **пересоздать** систему управления операционным риском с включением в неё процессов управления рисками ИБ и ИС с нуля;
  - **надстроить** процессы управления рисками ИБ и ИС над существующей системой управления операционным риском.
- **При реализации** системы управления рисками ИБ и ИС 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