Банк России

ОРГАНИЗАЦИЯ КИБЕРУЧЕНИЙ НА ОСНОВЕ АНАЛИЗА СЦЕНАРИЕВ АТАК – ПОДХОДЫ БАНКА РОССИИ

ДЕПАРТАМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
БАНКА РОССИИ

2020 г.

Основные направления развития ИБ КФС

Обеспечение информационной безопасности и киберустойчивости в целях финансовой стабильности каждой организации финансового рынка

Обеспечение операционной надежности и непрерывности деятельности организаций кредитно- финансовой сферы

Противодействие компьютерным атакам, в том числе при использовании инновационных финансовых технологий

Защита прав потребителей финансовых услуг

Киберучения

Цель: оценка способности финансовых организаций обеспечивать осуществление деятельности, связанной с предоставлением финансовых или информационных услуг, путем реализации мер, направленных на противодействие угрозам и киберустойчивость

Проведение стресс-тестирования финансовых организаций по вопросам ИБ

Риск-профилирование

Повышение готовности финансовой организации к выявлению рисков и противодействию угрозам в части обеспечения киберустойчивости

Банк России

Как это работает

- Типовые бизнес-процессы
- АСОИ. Инциденты поднадзорной
- Данные проверок
- Досье поднадзорной

1

Предпроверочная подготовка

2

Идентификация особенностей бизнес-процесса

3

Корректировка риск-ориентированного задания с учетом данных об особенностях бизнес-процесса

4*

Проверка в части процедур реагирования и восстановления

5*

Проверка в части оценки уровня управления бизнес-функциями, переданными на аутсорсинг

6*

Проверка в рамках управления риском реализации информационных угроз

Риск-профиль

* - Базельский комитет по банковскому надзору. Стандарт по операционной устойчивости «Principles for operational resilience»

Аналитика атак

А Экспертный анализ информации об инцидентах, атаках, уязвимостях, характерных для вида деятельности (по бизнес-процессу)

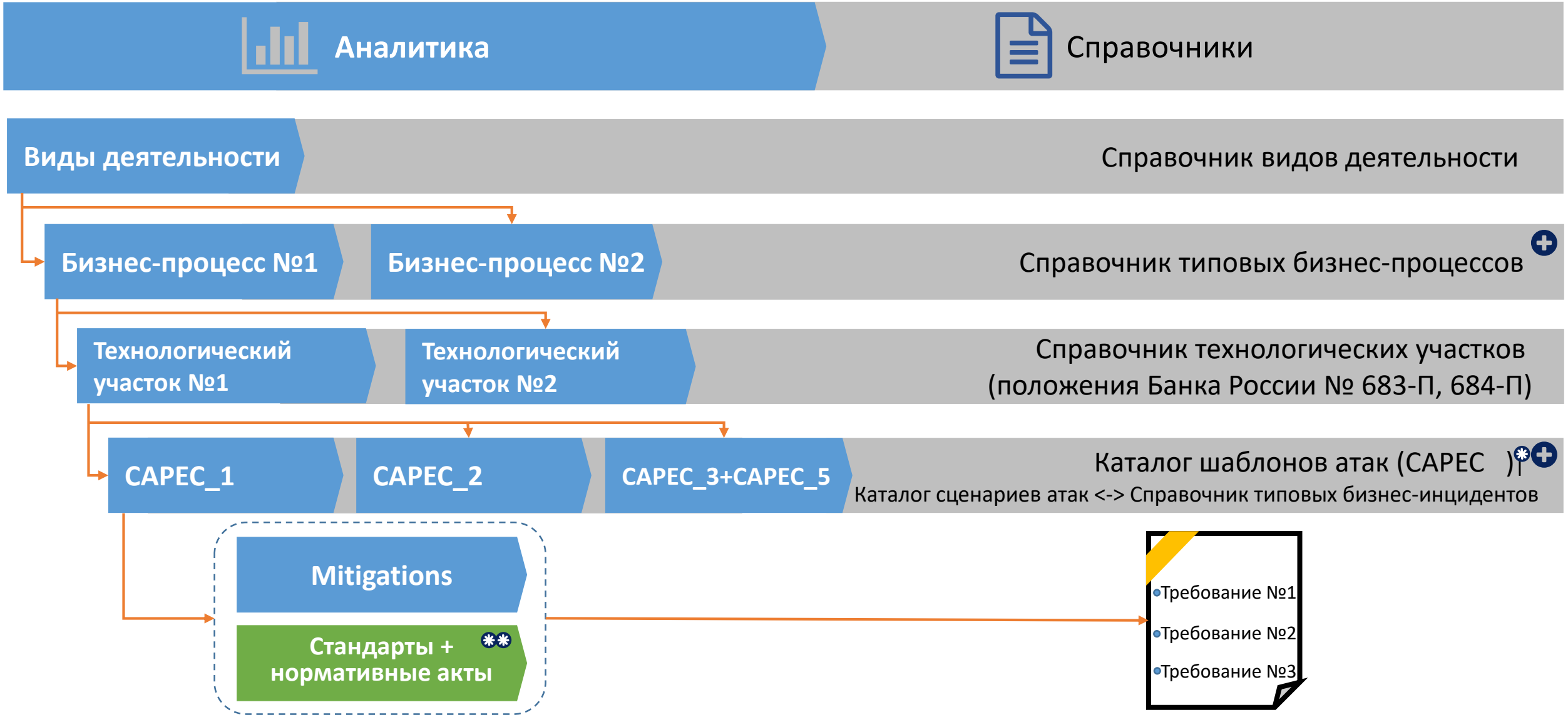
Б Разбор конкретного инцидента/бизнес-инцидента

Расширение состава предоставляемой информации*

* - по СТО БР БФБО-1.5-2018

Банк России

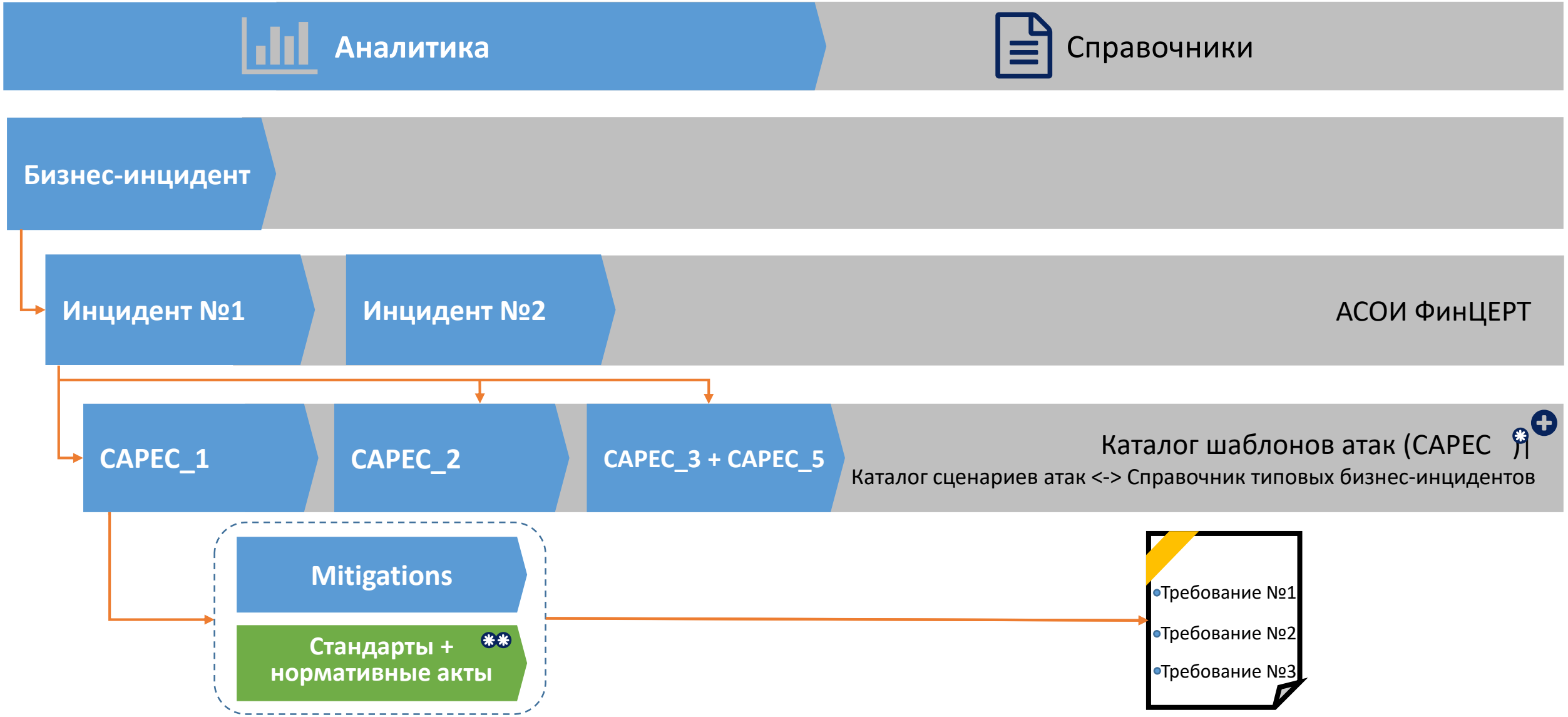
Анализ сценариев атак по бизнес-процессу



- www.capec.mitre.org
-ГОСТ 57580, Профиль защиты ППО, нормативные акты
- пополняется в рамках киберучений

Банк России

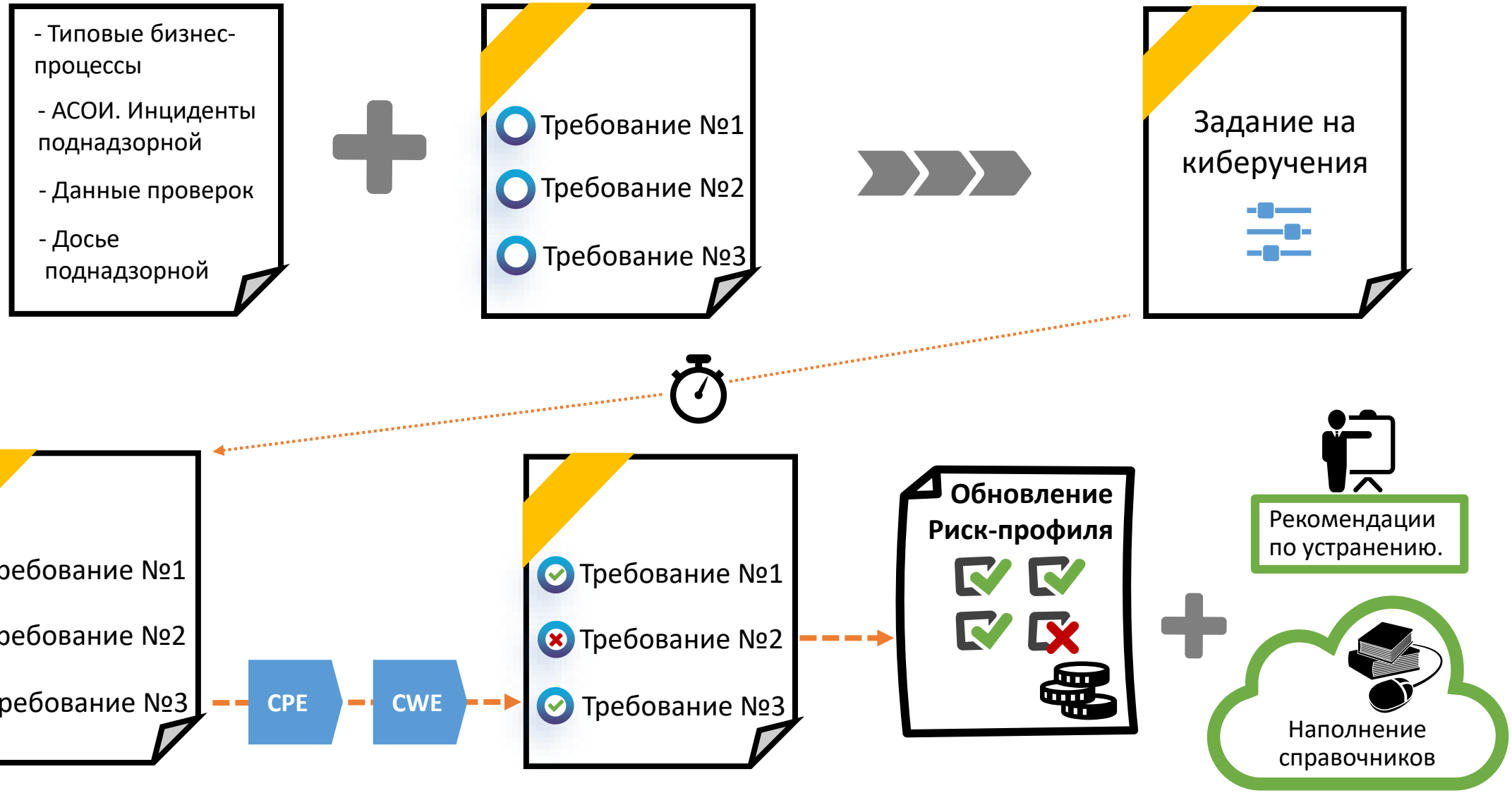
Анализ сценариев атаки по инциденту



- www.capec.mitre.org
-ГОСТ 57580, Профиль защиты ППО, нормативные акты
- пополняется в рамках киберучений

Банк России

Киберучения



Итог

Консультативный надзор: адресные проверки, точная оценка рисков

Обоснованное применение мер защиты (по итогам киберучений**)**

Результаты риск-ориентированного надзора, понятные для бизнеса

Банк России

СПАСИБО ЗА ВНИМАНИЕ

Пункт приема корреспонденции:
Москва, Сандуновский пер., д. 3, стр. 1, телефон +7 495 621-09-61
Почтовый адрес: 107016, Москва, ул. Неглинная, д. 12
Контактный центр: 8 800 250-40-72, +7 495 771-91-00
Факс: +7 495 621-64-65, +7 495 621-62-88
Сайт: www.cbr.ru
Электронная почта: cbr@cbr.ru