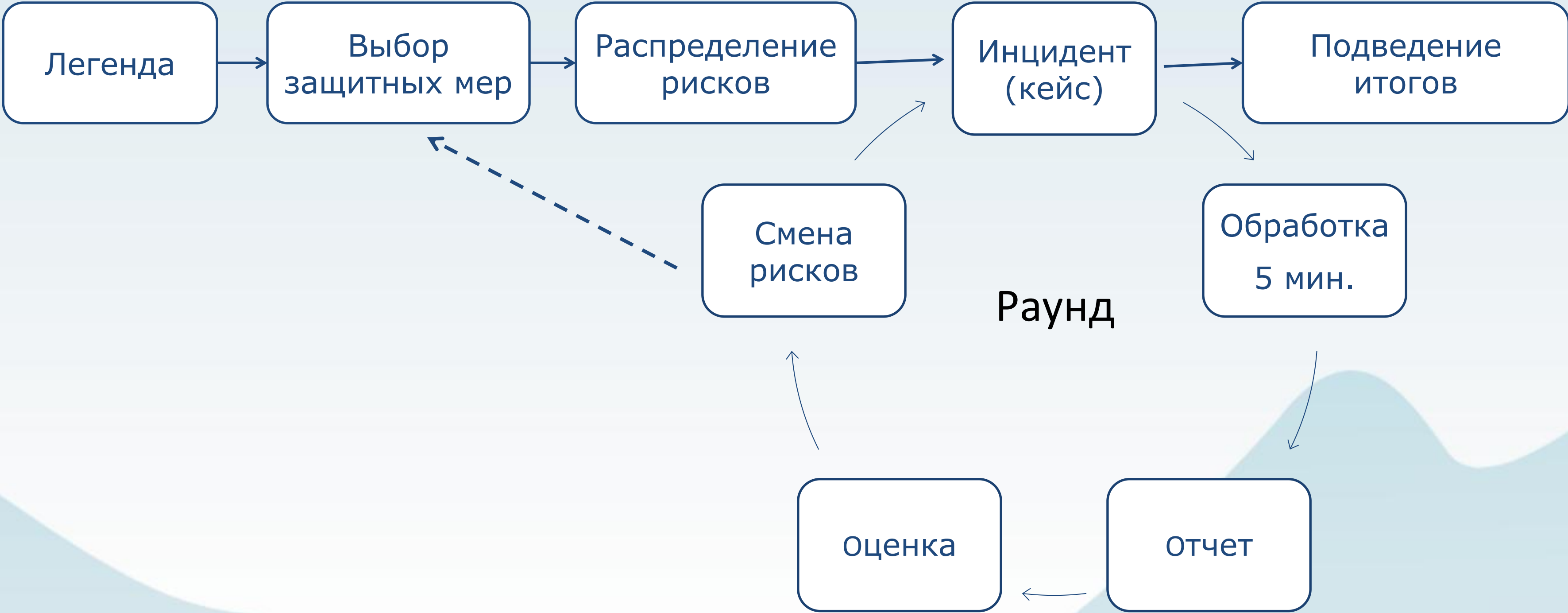


Правила

- 1.** У всех команд одинаковая легенда, но разные:
 - Возможности (защитные меры)
 - Обстоятельства (риски)
- 2.** 12 раундов (инцидентов)
После 4 раунда пройдет модернизация системы защиты
- 3.** Задача команды в каждом раунде:
Составить и презентовать план действий по реагированию
- 4.** По завершении раунда:
Команды голосуют за выступления друг друга (0-5 баллов)
Команды передают по кругу 1 любую карточку риска

Цель - набрать максимальное число баллов

Правила



Задание № 0

Название для команды мечты?

Напишите ваше название и названия других команд

Команда:

Команда/раунд	1	2	3	4	5	6	7	8	9	10	11	12	ИТОГО

Можно поставить от 0 до 5 баллов

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ПРОФИ



Выбор защитных мер

1. У каждой меры есть стоимость - от 1 до 5 баллов
2. У команды 15 баллов на счете
3. Обведите меры, которые решили внедрить
4. Их суммарная стоимость не должна превышать 15

Защитные меры

Команда:

Всего баллов: **15**

DLP	3	Обучение пользователей	1
SIEM	3	Соглашения о конфиденциальности	1
Антивирус	2	Двухфакторная аутентификация	3
Резервное копирование	2	Безопасная настройка конфигураций ОС и ПО	1
Межсетевой экран	2	Шифрование съёмных носителей	3
Сканер безопасности	2	Подписка на КодИБ Академия	1
Внедрение DevSecOps	3	Аттестация системы	2
РАМ	3	Сегментирование сетей	1
Режим КТ	2	Процесс управления рисками	1
Подписка на SOC	4	Система контроля конфигураций	2
DCAP	3	Система мониторинга ИТ инфраструктуры	2

Выбор защитных мер

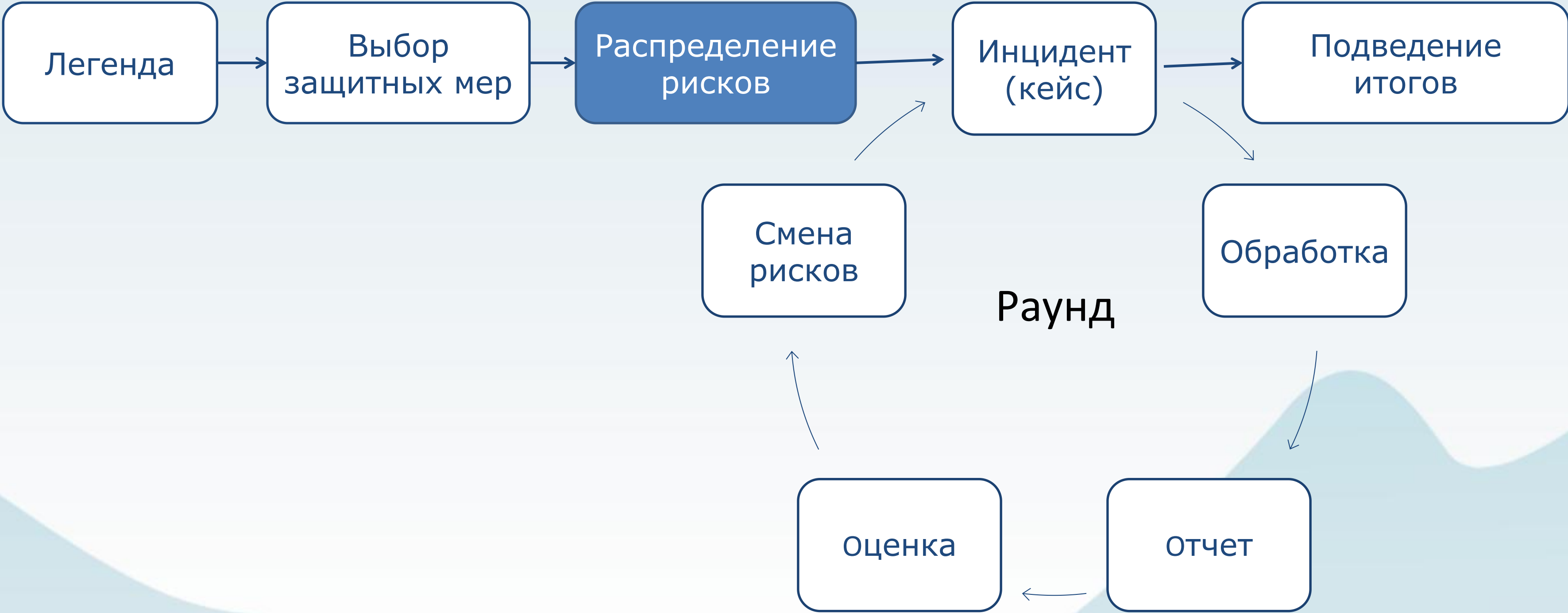
Защитные меры

Команда:

Всего баллов: **15**

DLP	3	Обучение пользователей	1
SIEM	3	Соглашения о конфиденциальности	1
Антивирус	2	Двухфакторная аутентификация	3
Резервное копирование	2	Безопасная настройка конфигураций ОС и ПО	1
Межсетевой экран	2	Шифрование съёмных носителей	3
Сканер безопасности	2	Подписка на КодИБ Академия	1
Внедрение <u>DevSecOps</u>	3	Аттестация системы	2
PAM	3	Сегментирование сетей	1
Режим КТ	2	Процесс управления рисками	1
Подписка на SOC	4	Система контроля конфигураций	2
DCAP	3	Система мониторинга ИТ инфраструктуры	2

Правила



Карточки рисков

- Действуют постоянно
- Можно нейтрализовать в рамках 1 раунда, потратив баллы
- Можно передать в конце раунда

Карточка риска




Бухгалтер уехал
Финансовые опера
Митигация: Выз
отпуска

Карточка риска



В процессе отчистки се
то пошло не так. досту
невозможен.
Митигация: Ручной прос

Карточка риска



У сотового оператора солнечные бури.
Связь с причастными к инциденту не
работает.
Митигация: Общение по почте

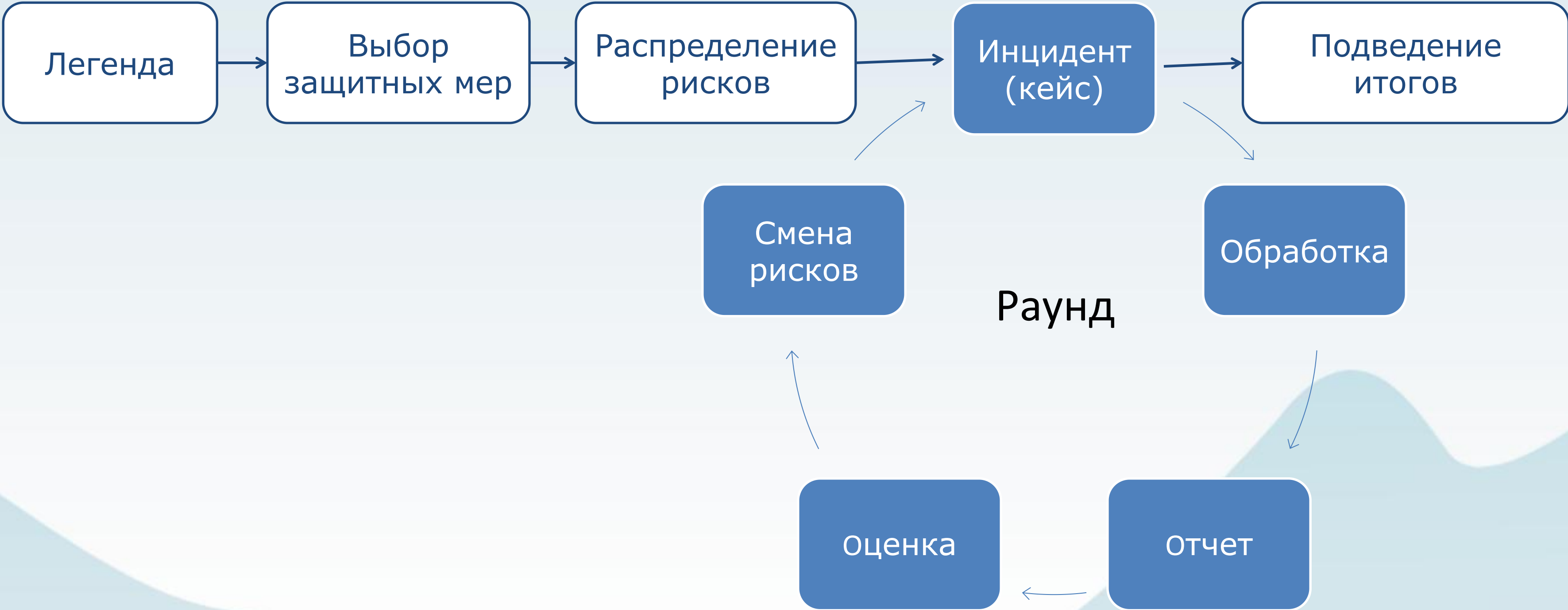
-3

Карточки рисков с действием

- Действуют 1 раз каждый раунд
- Можно нейтрализовать в рамках 1 раунда, потратив баллы
- Можно передать в конце раунда



Правила



План действий

План действий

Раунд _____

Команда _____

1. _____

2. _____

3. _____

4. _____

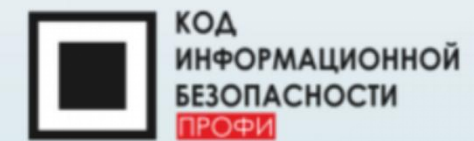
5. _____

Голосование

Команда:

Команда/раунд	1	2	3	4	5	6	7	8	9	10	11	12	ИТОГО

Можно поставить от 0 до 5 баллов



Кейс 0

Сотрудник сообщил что на его экране странное сообщение и ничего не работает

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

a8w8ff-KM4ubE-f2GcKZ-uKZpWW-Z8mbaU-5tXMH5-zjxgZF-yXqHPB-K3z46v-eS6qZt

If you already purchased your key, please enter it below.

Key:

Кейс 0

Сотрудник сообщил что на его экране странное сообщение и ничего не работает

```
Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
deryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
wowsmith123456@posteo.net. Your personal installation key:

a8w8ff-KM4ubE-f2GcKZ-uKZpWW-Z8mbaU-5tXMH5-zjxgZF-yXqHPB-K3z46v-eS6qZt

If you already purchased your key, please enter it below.
Key:
```

Ваши защитные меры

- DLP
- Соглашения о конфиденциальности
- Аттестация системы
- Система контроля конфигураций
- Межсетевой экран
- Антивирус
- DCAP

Ваши риски

- Финансовые операции невозможны
- Архив DLP уничтожен
- Связь с причастными к инциденту не работает