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

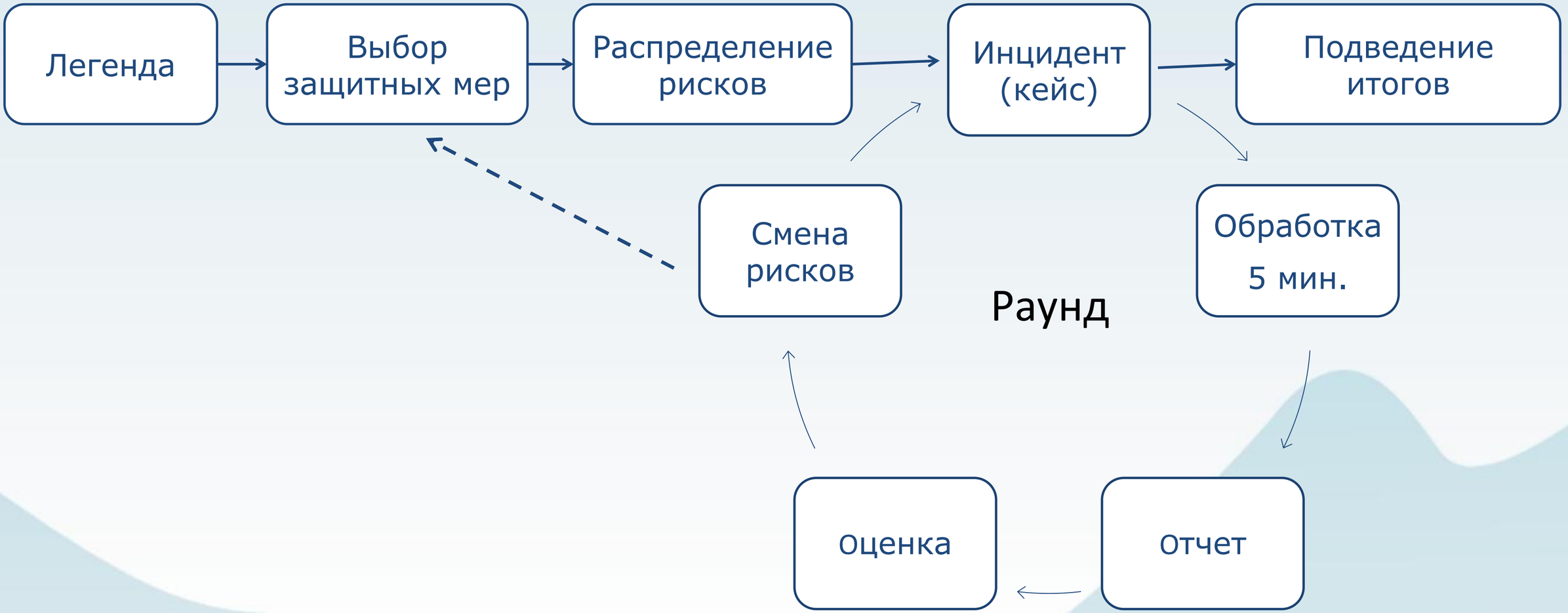
4. По завершении раунда:

Команды голосуют за выступления друг друга (0-5 баллов)

Команды передают по кругу 1 любую карточку риска

Цель - набрать максимальное число баллов

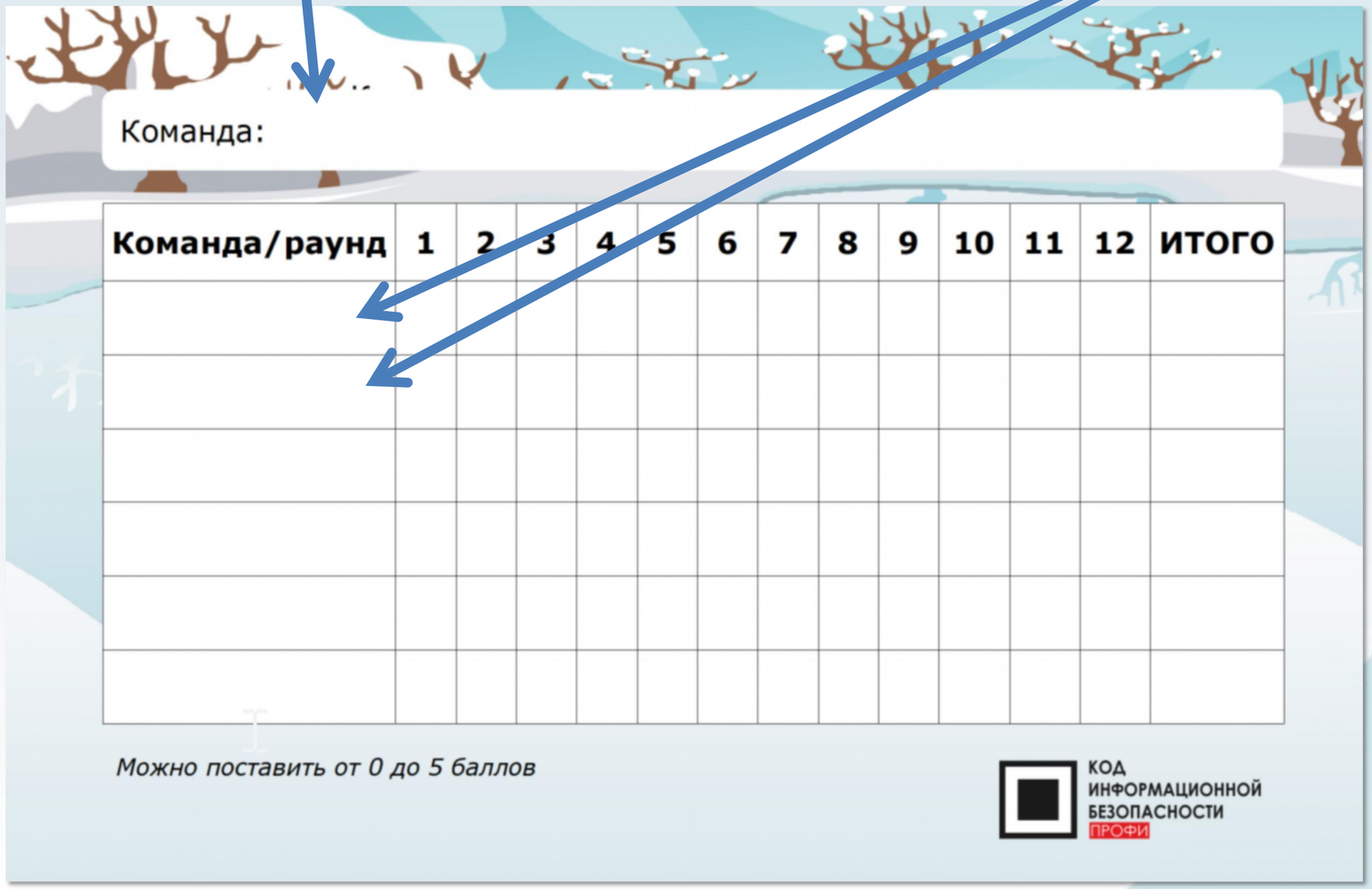
Правила


Легенда
Выбор защитных мер
Распределение рисков
Инцидент (кейс)
Подведение итогов
Смена рисков
Обработка 5 мин.
Раунд
Оценка
Отчет

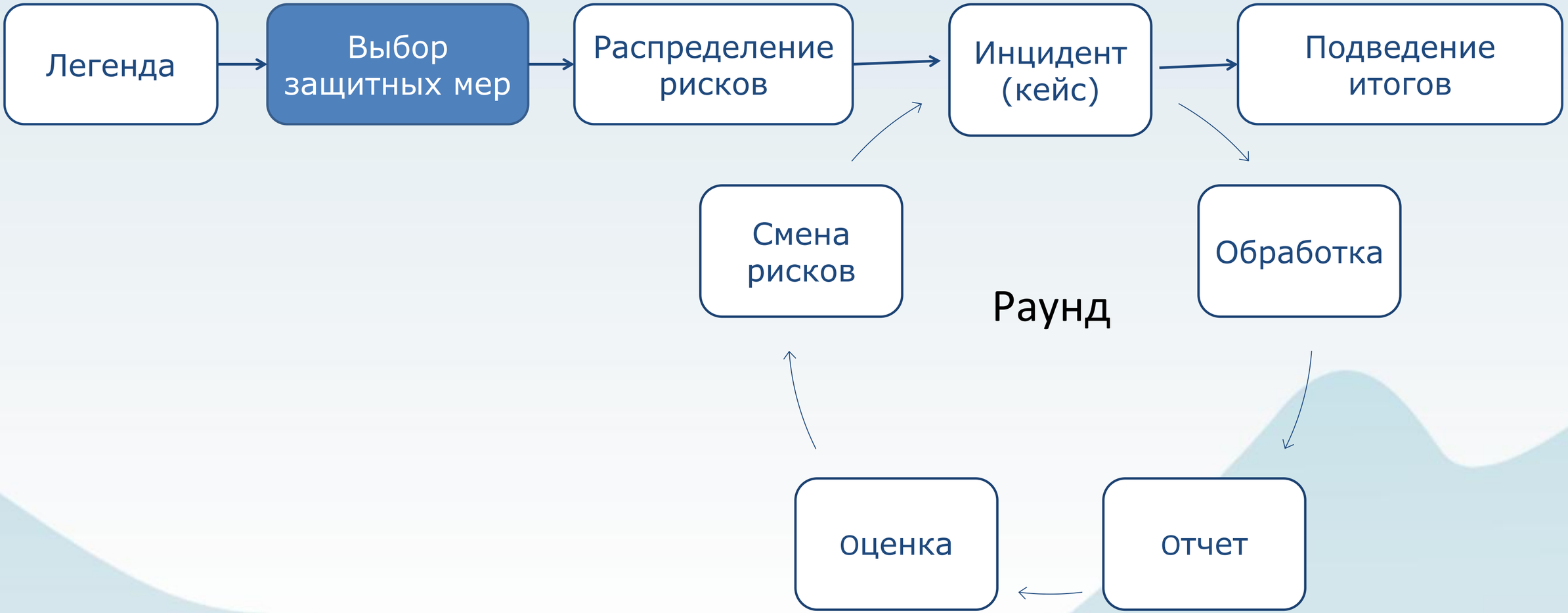
Задание № 0

Название для команды мечты?

Напишите ваше название и названия других команд



Правила


Легенда
Выбор защитных мер
Распределение рисков
Инцидент (кейс)
Подведение итогов
Обработка
Отчет
Оценка
Смена рисков
Раунд

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
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

Выбор защитных мер

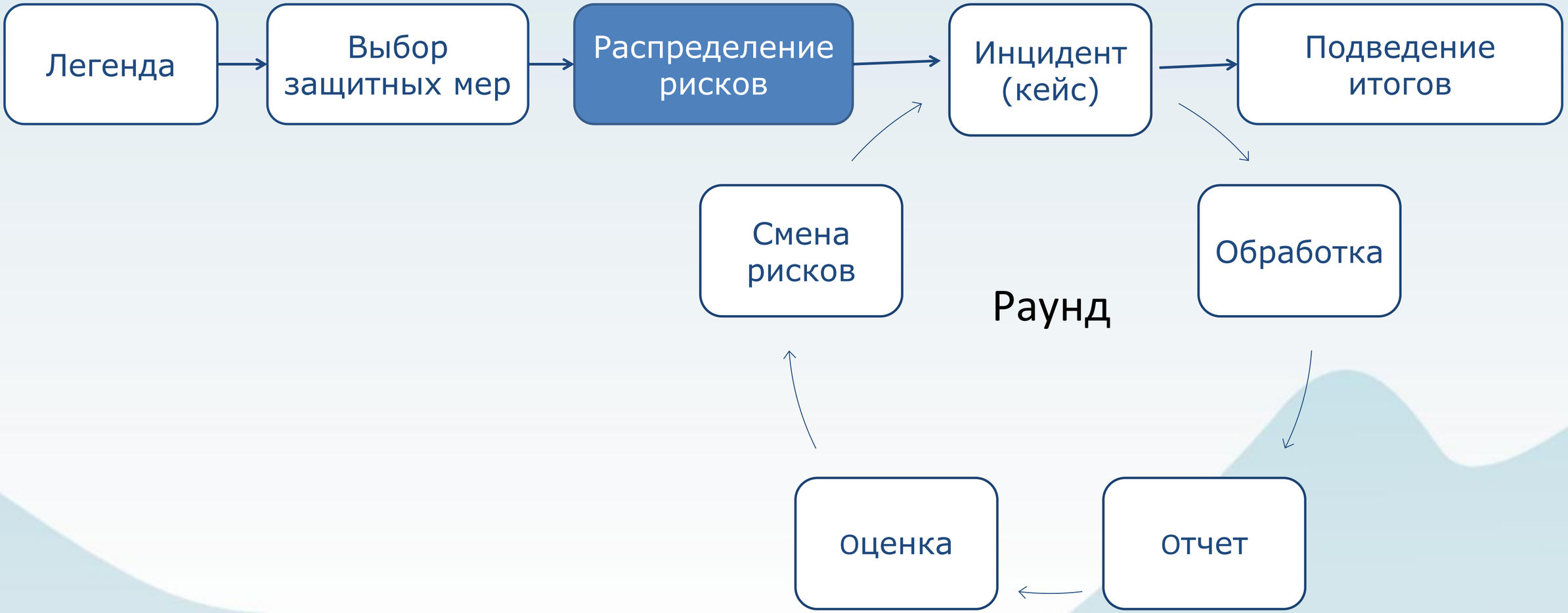
Защитные меры

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 DevSecOps	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


Легенда
Выбор защитных мер
Распределение рисков
Инцидент (кейс)
Подведение итогов
Обработка
Отчет
Оценка
Смена рисков
Раунд

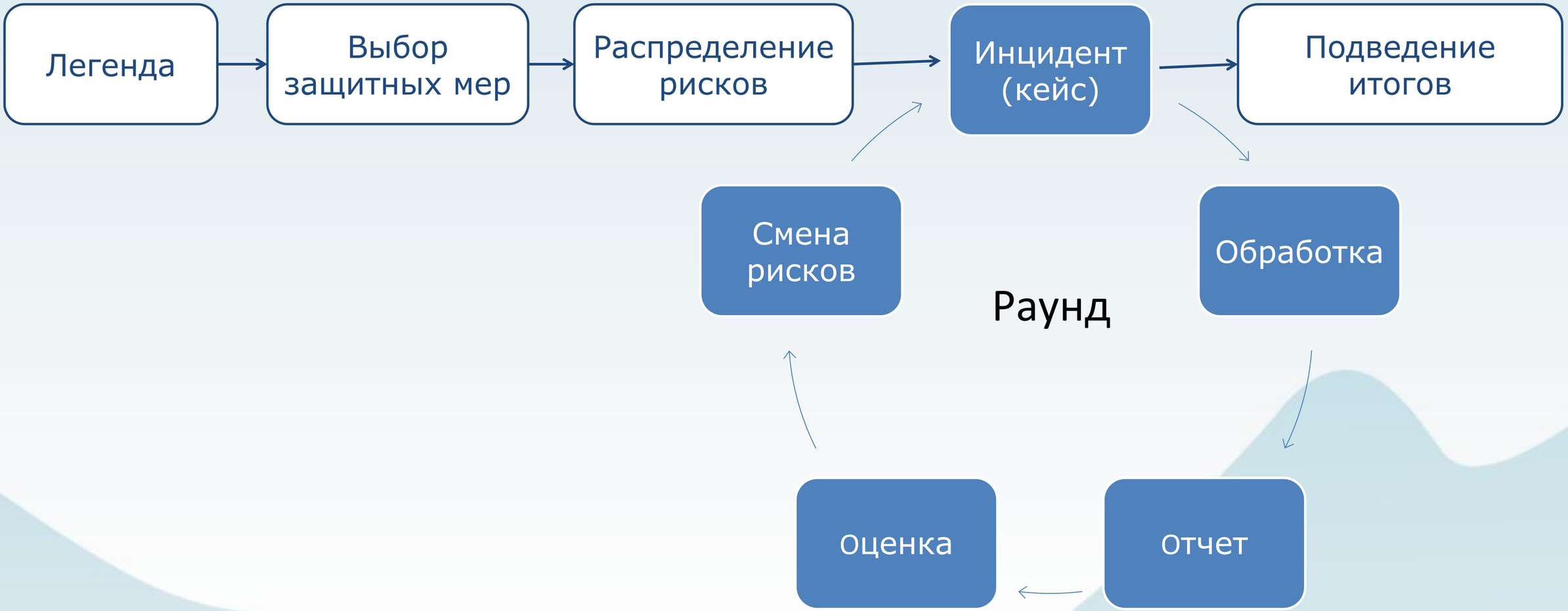
Карточки рисков

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

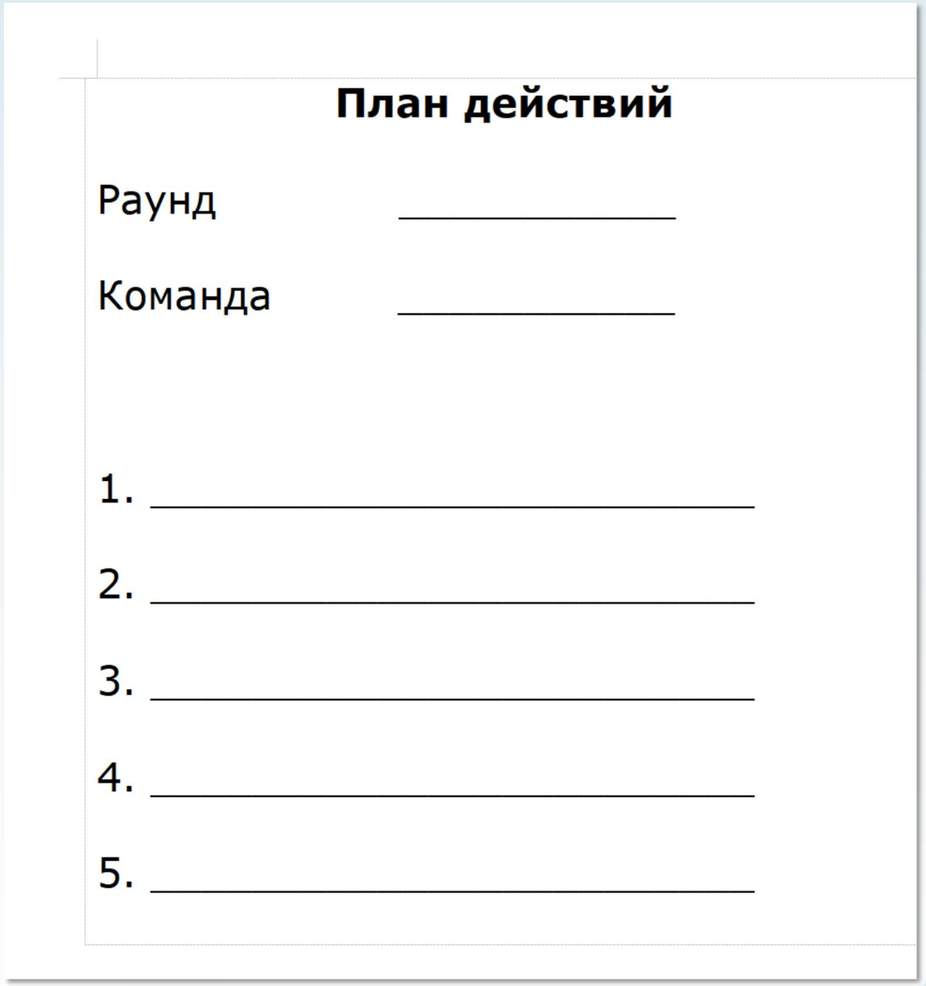
Карточки рисков с действием

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

Правила


Легенда
Выбор защитных мер
Распределение рисков
Инцидент (кейс)
Подведение итогов
Смена рисков
Обработка
Раунд
Оценка
Отчет

План действий



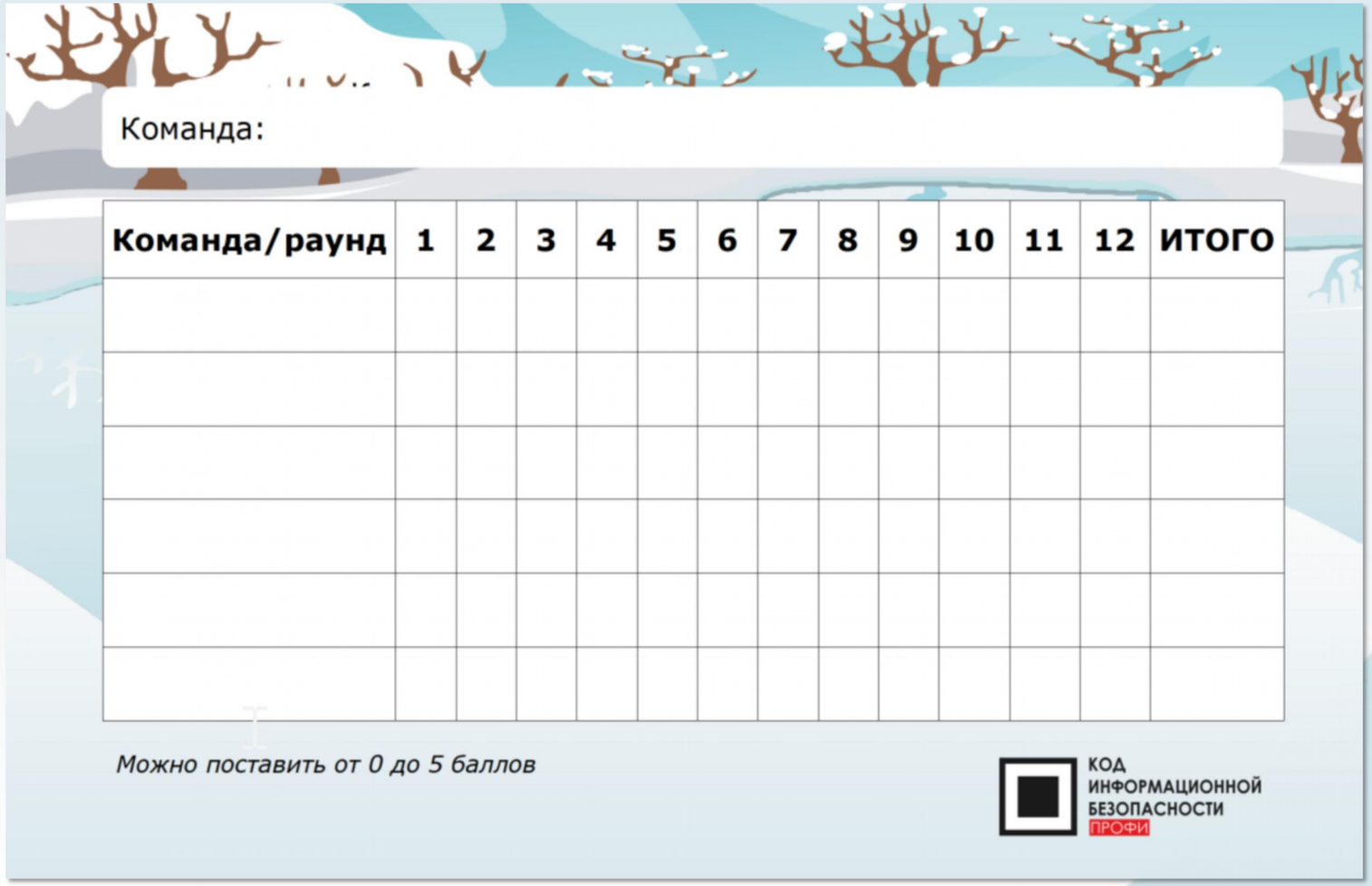
План действий

Раунд _____

Команда _____

1. _____
2. _____
3. _____
4. _____
5. _____

Голосование



Команда:

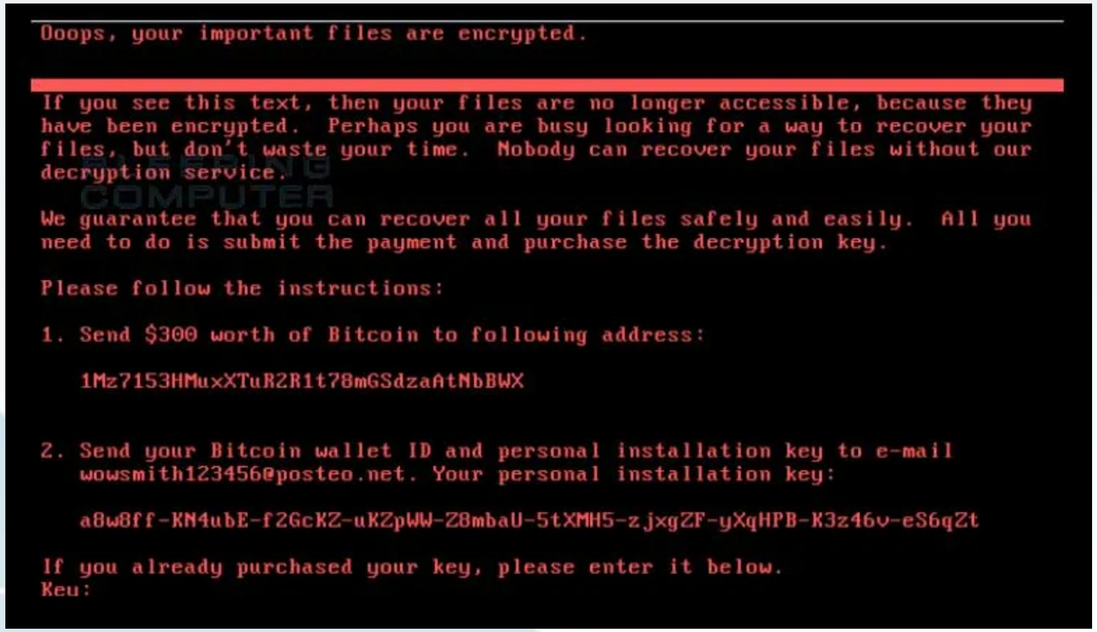
Команда/раунд	1	2	3	4	5	6	7	8	9	10	11	12	ИТОГО

Можно поставить от 0 до 5 баллов

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОФИ

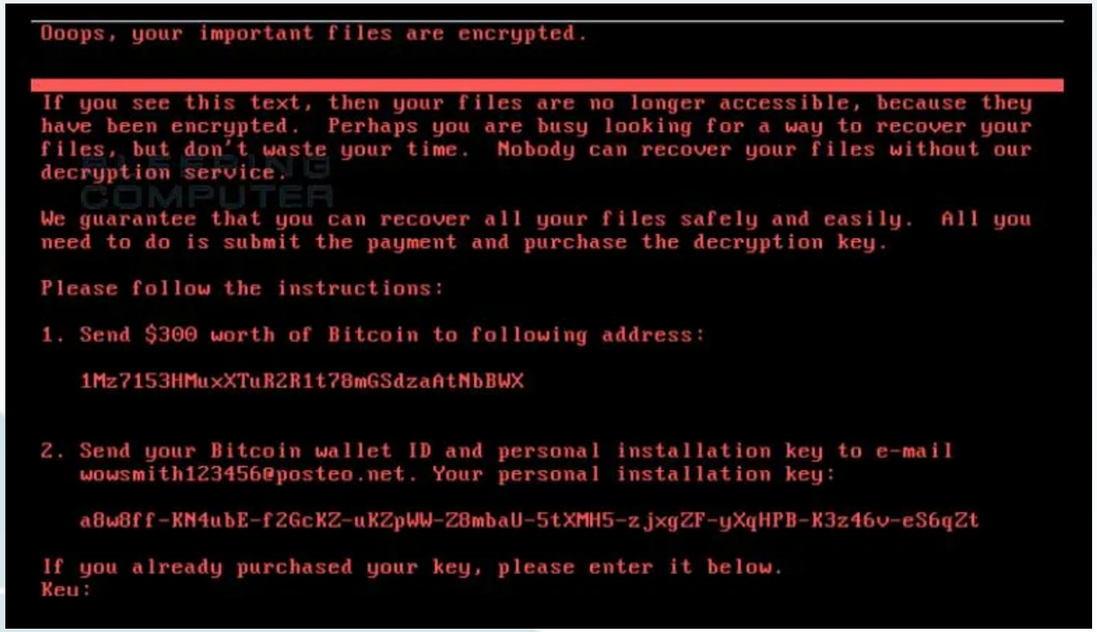
Кейс 0

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



Кейс 0

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



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