КОД ИБ | Санкт-Петербург

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как провести штабные киберучения?

21.04.2022

Всеслав Соленик

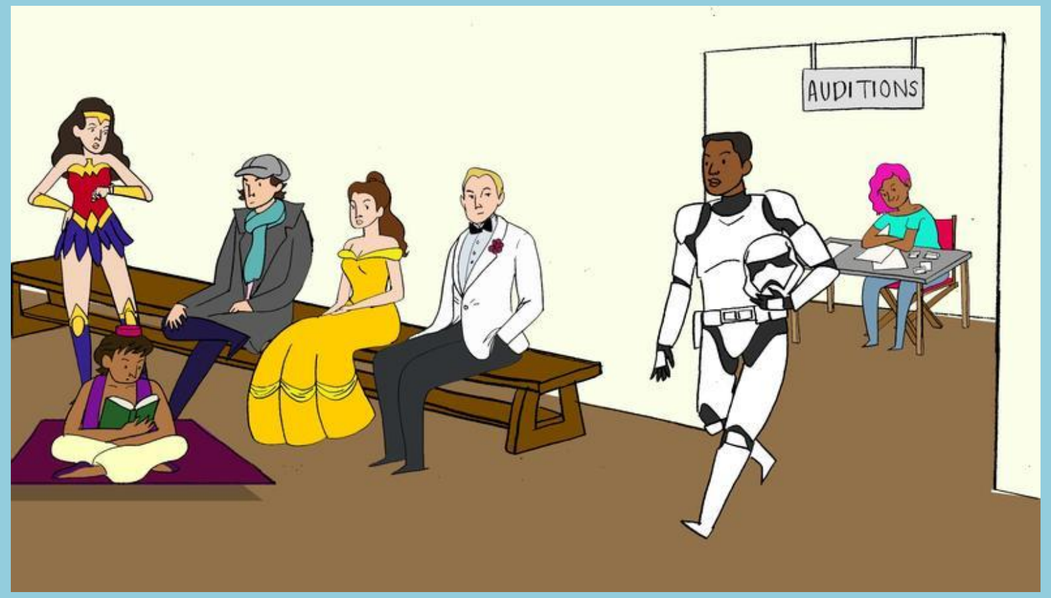
Коротко обо мне

- Окончил ИКСИ, факультет информационной безопасности.
- С 2010 года занимал экспертные и руководящие позиции (CISO, CSO, BCP Manager) в финансовой сфере.
- С 2019 года - директор центра экспертизы российского вендора R-Vision, где помогаю клиентам компании строить и автоматизировать процессы информационной безопасности на базе продуктов R-Vision, а также в целом развивать отечественный рынок ИБ.
- Активный участник российского сообщества экспертов по информационной безопасности. Спикер-практик, автор статей и выступлений на многих площадках России и СНГ.

РАЗМИНКА

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ И HR



«Представьте, что в разгар рабочего дня вам звонит админ Core-системы и говорит, что наблюдает как файлы на сервере на его глазах превращаются в «абракадабру».

Ваши действия?

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ И HR

× Забуду уведомить пользователей

× Отключу и забуду о «бизнесе»

× Не уточню, что за сервер, его профиль

× Восстановлю из бэкапа – победа!

× Не догадаюсь о средствах мониторинга

× Забуду вернуть в изначальное состояние

× Снова забуду уведомить пользователей

× Не проведу расследование пути заражения

× Никаких мер по неповторению

× Не подготовлю отчет для руководства/регулятора

× …

× Не справлюсь с задачами специалиста по ИБ

Всякий ли инцидент - инцидент?

- ? Утекли или зашифрованы личные файлы первого лица Компании
- ? Студент нашел дыру и опубликует на «Хабре», если не закрыть в течение недели
- ? Пентестеры успешно взломали (или «перестарались»)
- ? Первое лицо договорилось с ИТ об упрощении аутентификации
- ? Сбой системы был в нерабочее время/в тестовой среде или «без последствий»
- ? Антивирус нашел «warning» с подозрением на троян
- ? Вовремя не устранили найденные сканером критичные уязвимости

А вы говорите, оценка рисков – методологически сложна… ☺

КИБЕРУЧЕНИЯ. КЕЙС

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Атака на Garmin

$10M предположительно выплачен выкуп

1 неделя – частичная недоступность сервисов Garmin, включая носимые устройства, заводы, колл-центры, авиа и морскую навигацию

Санкции властей США за сотрудничество с киберпреступниками

Посредник для уплаты выкупа (Arete IR)

WastedLocker – используемый шифровальщик EvilCorp

Фишинг – предполагаемый способ заражения инфраструктуры

$...

Репутационные потери

КИБЕРУЧЕНИЯ. ТЕОРИЯ

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Что называют киберучениями?

Штабные игры

Для менеджмента, команды ИБ и ИТ или соревнования команд

CTF

Техническое соревнование команд по реализации задуманных организаторами атак/реагирования

Кибер-полигоны

Техническое real-time соревнование команд на симуляции «боевой» инфраструктуры

Кому и зачем нужны штабные киберучения?

- Участники: ИБ/ИТ и руководители структурных подразделений
  - Топы, ИТ, АХО, финансы/бухгалтерия, юристы, маркетинг/PR, продажи, производство, колл-центр

- «Пройти» через инцидент ИБ вместе с командой руководителей компании
  - Погружение других функций в ваш контекст
  - Безопасность – не только ваша потребность, спросите у Маслоу ☺
  - Тимбилдинг и повышение статуса в глазах руководства, эффект совместной работы над задачей
  - Прокачка soft skills

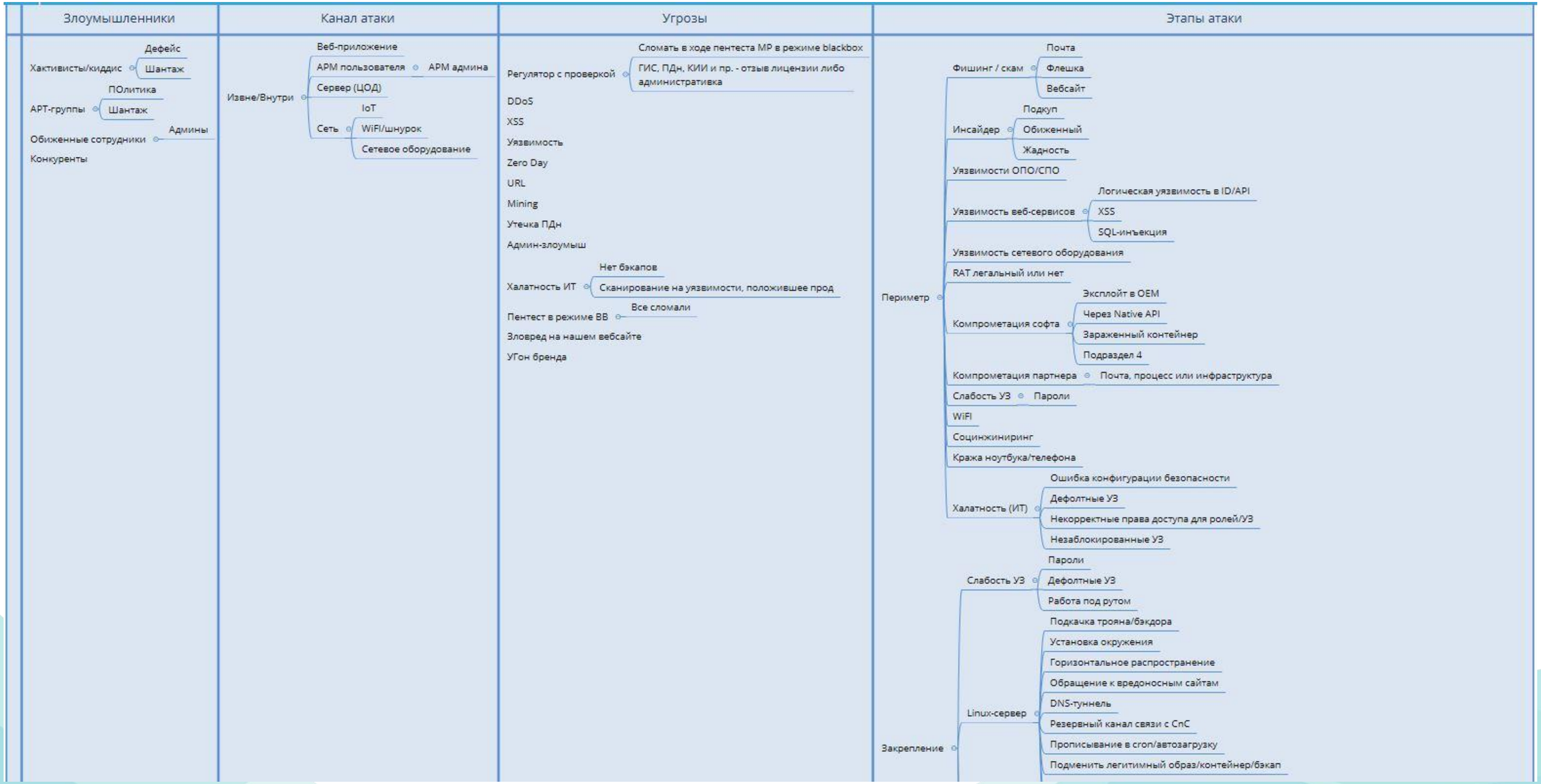
- Вы обнаружите, что многое можно подготовить заранее – и будете лучше готовы к инциденту, когда он наступит

- Вы обнаружите, что не только от вашей команды зависит успешное реагирование на инцидент ИБ

Как организовать киберучения?

- Подготовить интересный и актуальный сценарий. Заранее. Можно с аутсорсом.
- Определить обязательных и опциональных участников, вовлечь их
- Первичные инструкции и регламент с четкими правилами
- Фасилитация и полная проработка всех веток и задач
- Саспенс, вбросы и динамика
- Выводы и **Action plan**
- Аналогия Crisis Exercise и BCP тест

Как придумать сценарий?



Кейсы, созданные трансформацией бизнеса

Переход на цифровые каналы и 24/7 доступность для партнеров и клиентов	Инциденты недоступности сервисов в любое время суток
Аутсорсинг «не-основных» бизнес процессов	Инциденты взаимодействия с третьими сторонами
Удаленные сервисы (биометрия для клиентов, работа из дома для сотрудников)	Инциденты удаленной авторизации и аутентификации, утечки данных
Фокус на скорости вывода сервисов на рынок	Инциденты, связанные с принятием рисков и недостаточной проработкой решений
Agile и DevOps в командах разработки Использование open source и западных продуктов	Инциденты, связанные с ошибками разработки и уязвимостями в приложениях
Централизация клиентских данных и «облака»	Инциденты массовых утечек

КИБЕРУЧЕНИЯ. ПРАКТИКА

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

О реагировании в SOC’ах

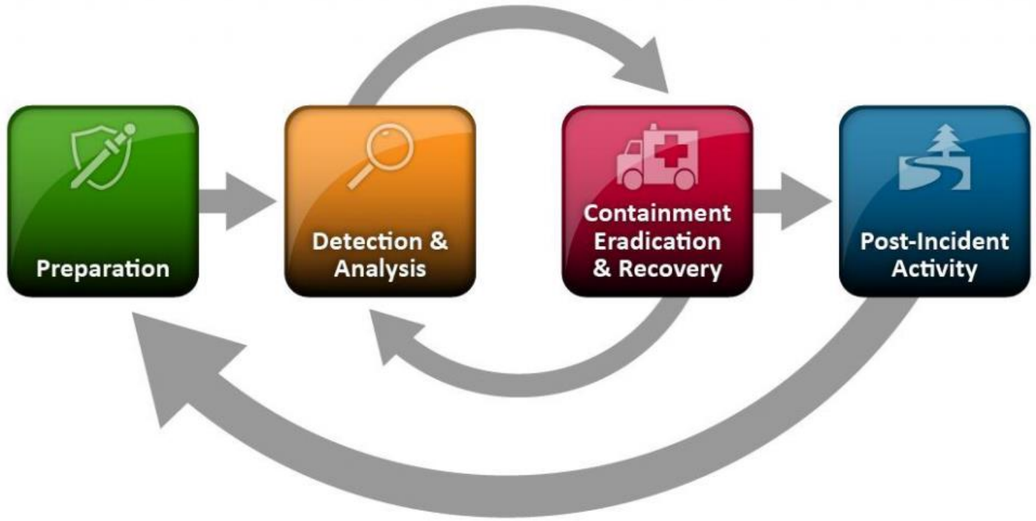
Инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность… © ГОСТ Р ИСО/МЭК 27001-2006

- Уведомление
- Локализация
- Внедрение мер
- Восстановление
- Расследование
- Отчетность

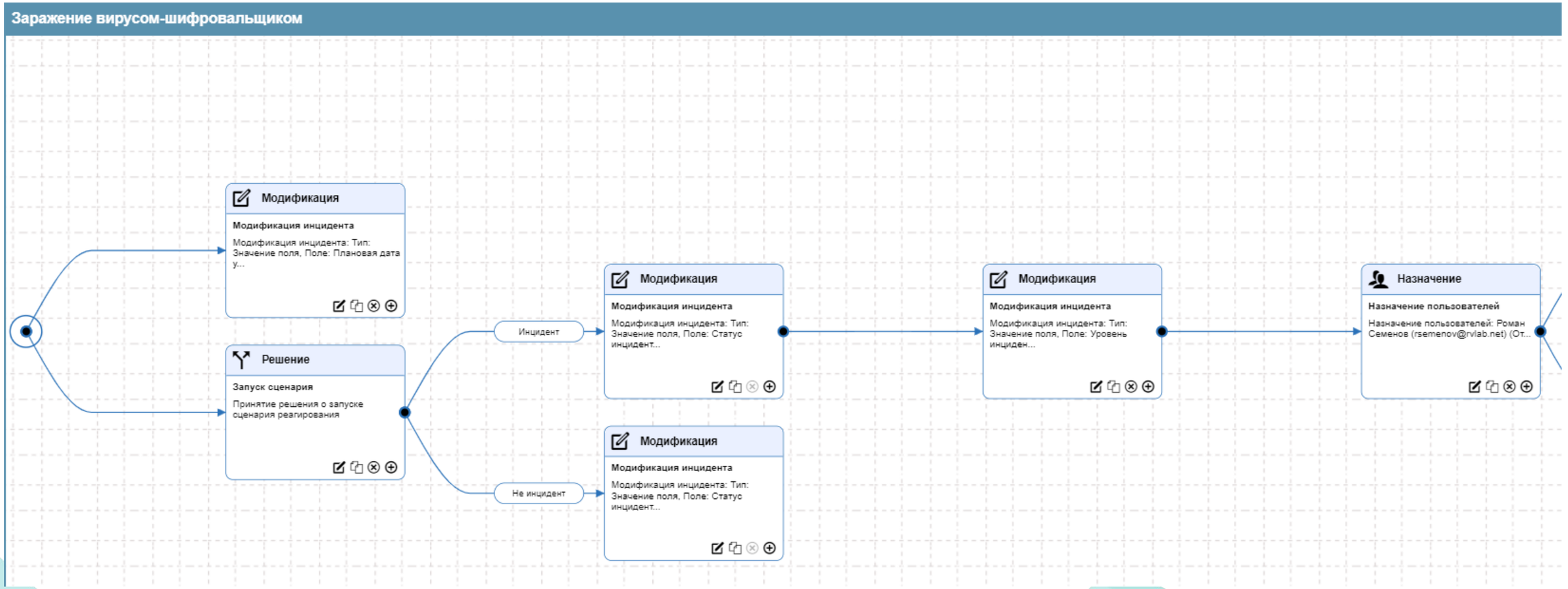
Порядок реагирования

Реагирование на инцидент подразумевает поиск ответов на следующие вопросы:

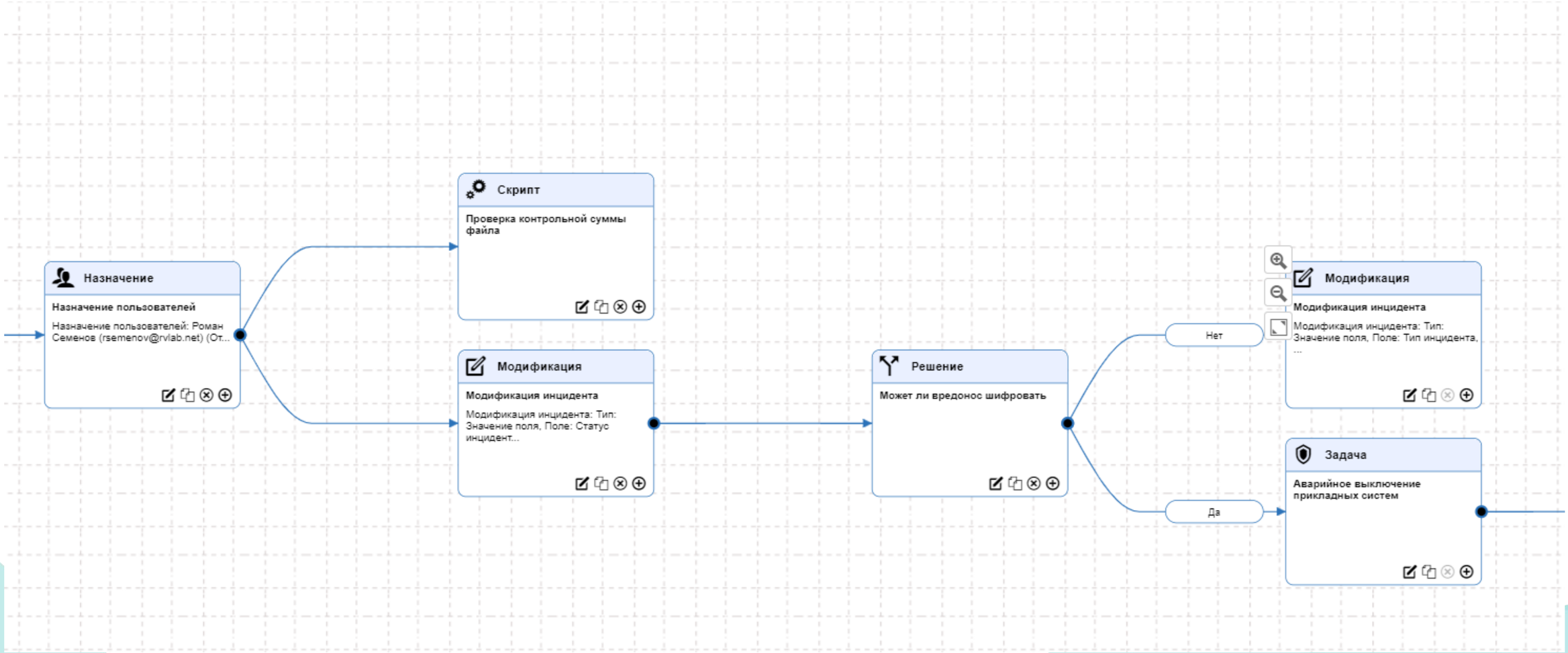
1. Кто ответственный? (рабочая группа и ответственный специалист)
2. Это точно инцидент? (проверка на false-positive)
3. Как остановить распространение инцидента? (локализация)
4. Как вернуться к нормальной работе? (ликвидация)
5. Почему произошел инцидент? (расследование)
6. Как не допустить в будущем? (Выводы)



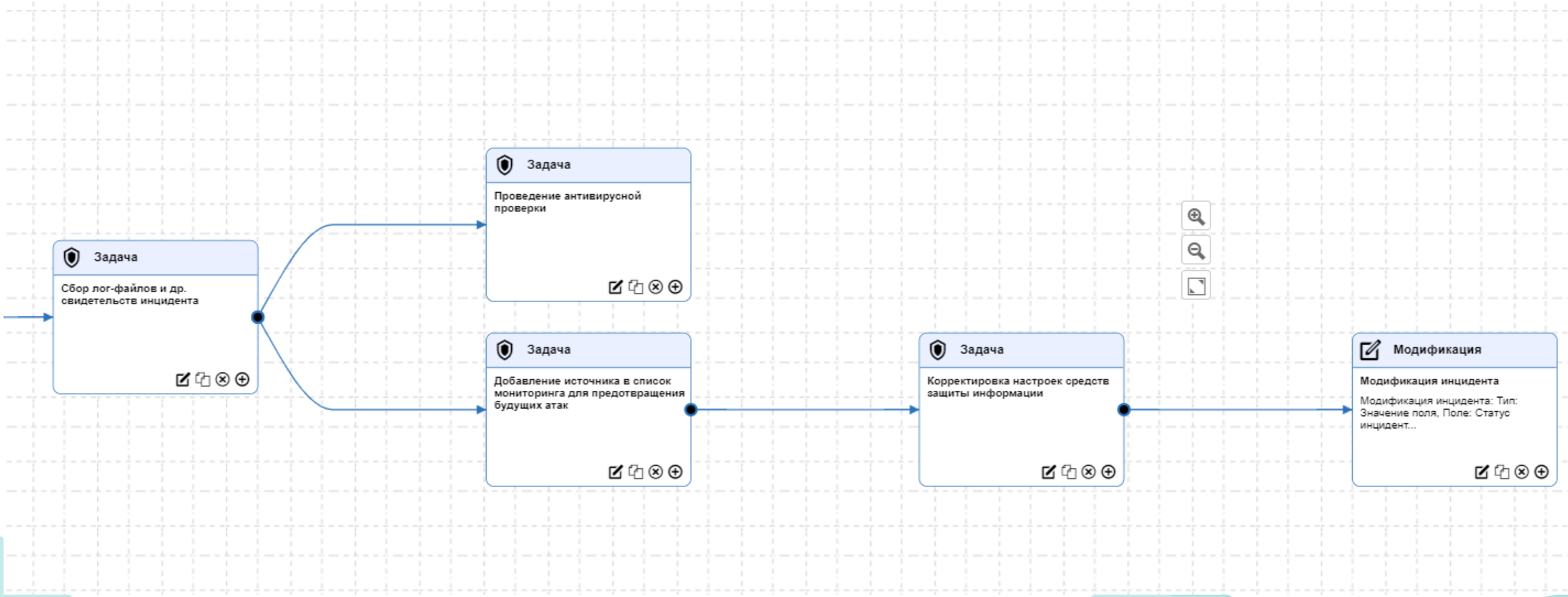
Пример плейбука по шифровальщику



Пример плейбука по шифровальщику



Пример плейбука по шифровальщику



Штабные киберучения!

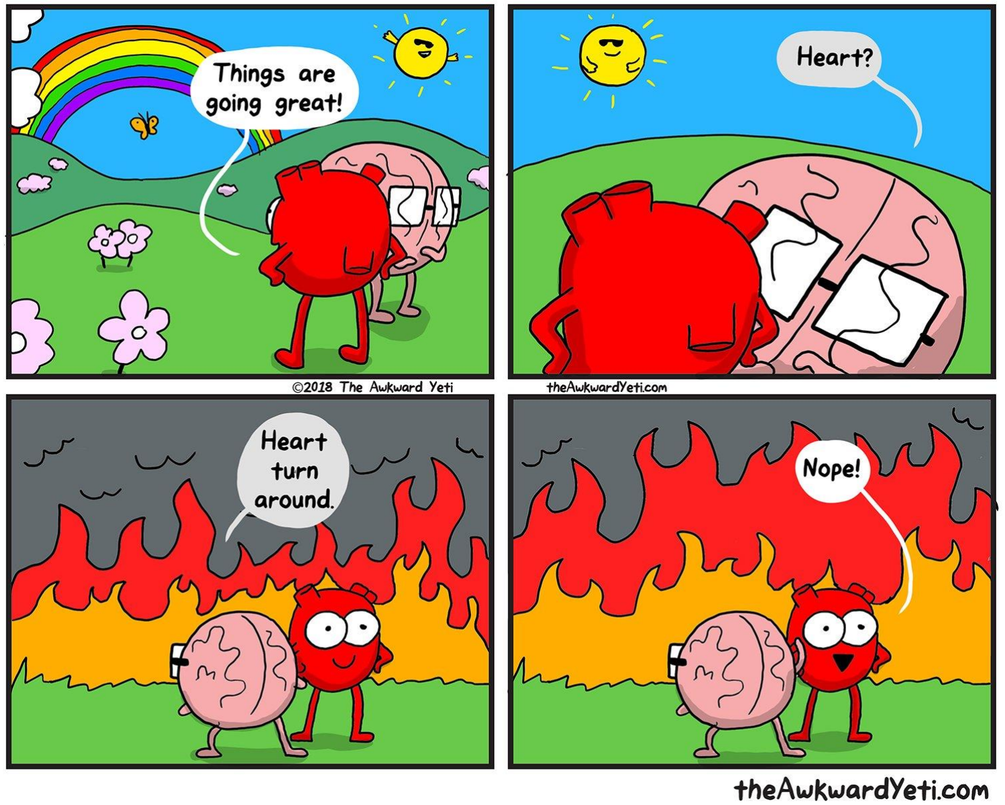
- Собираем **2** команды (по 10-12 человек).
    - Каждая команда готовит и описывает сценарий атаки. Время – 30-40 минут.
        - Раунд 1:
            - Команда 1 – «атакуют»,
            - команда 2 – «реагируют»,
        - Раунд 2: смена ролей.

**По итогам каждого раунда коротко Action Plan лично для себя и своей компании + обратная связь из зала.*

Штабные киберучения!

Не забудьте при подготовке сценария учений:

1. Подробное описание инцидента шаг за шагом – для исчерпывающих ответов на вопросы.
2. Подробная вводная, что произошло на момент начала симуляции,
3. Разбить симуляцию на несколько этапов развития инцидента с их описанием.
4. Определить для себя ключевые вехи реагирования.
5. Вовлеченные лица со стороны Компании – кто они?
6. Продумайте участие нескольких внешних акторов.
7. Дайте 1-2 неожиданных вводных.
8. Какие выводы вы считаете нужно сделать по итогам?



И еще пара советов:

- Не будьте банальными – мыслите смело.
- К инциденту всегда приводит как минимум 2-3 ключевых фактора.
- Не углубляйтесь в технические детали!

Готов ответить на ваши вопросы

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

СПАСИБО ЗА ВНИМАНИЕ!

ПОЧТА
vseslav.sol@gmail.com

ТЕЛЕФОН
+7 926 4515101