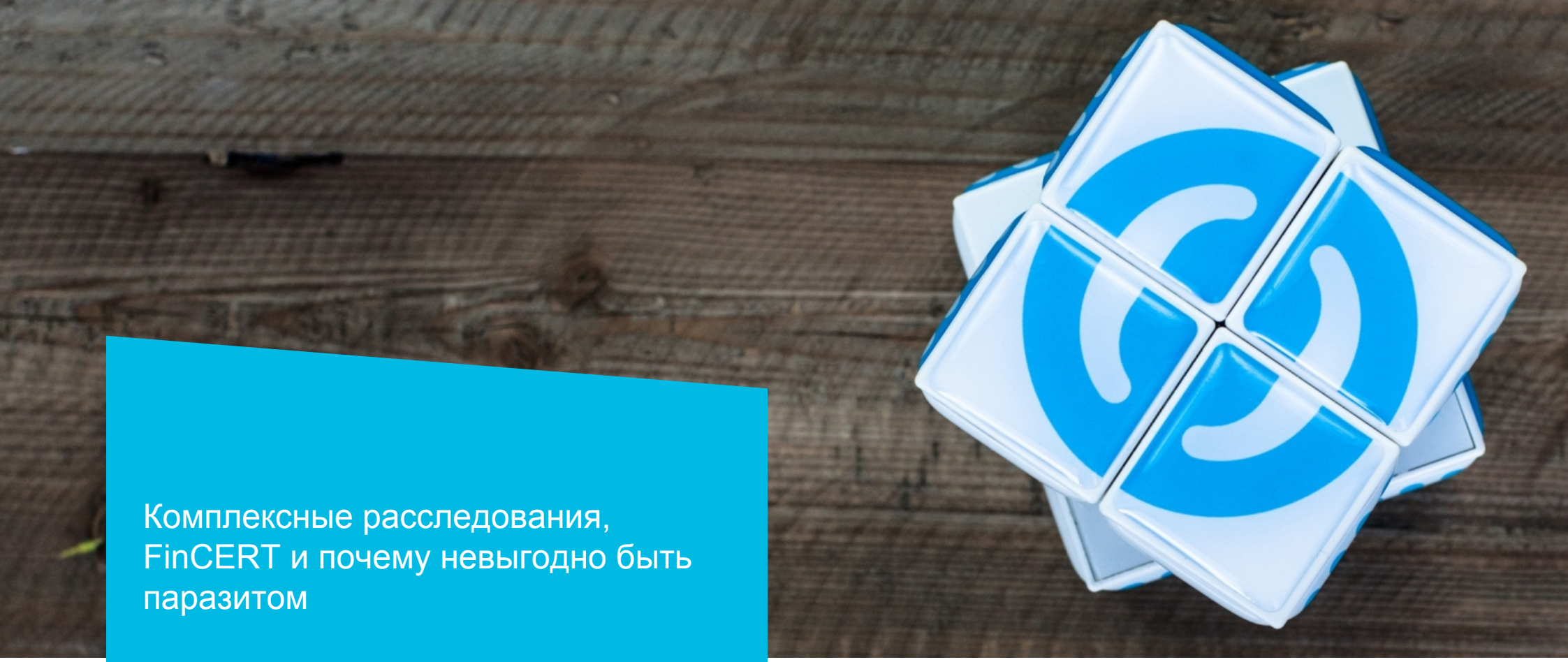


Комплексные расследования, FinCERT и почему невыгодно быть паразитом

В жизни всегда
есть место открытию

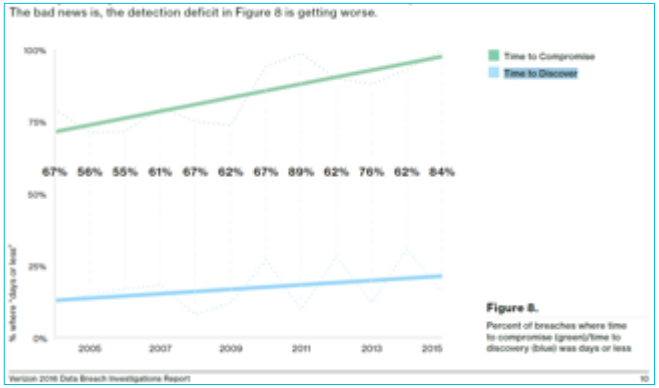
openbank.ru

открытие | БАНК

Актуальные проблемы информационной безопасности

ТРЕНДЫ 2017 ГОДА

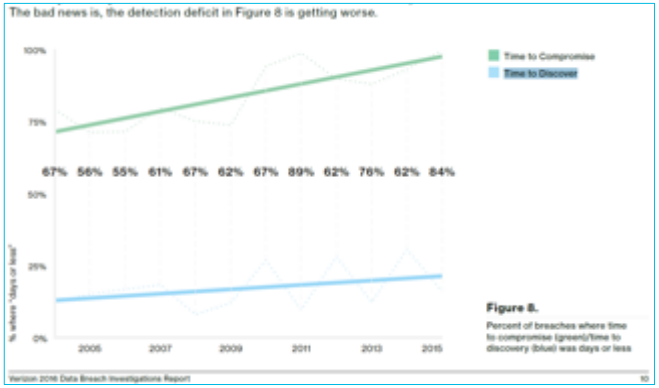
- Симметричный рост атак на клиентов банков и сами банки
- Пассивные закладки и короткие заражения (Crime-as-a-Service)
- Использование Internet of things в атаках
- Сигнатуры малоэффективны
- Поддельные сайты
- Рост времени обнаружения инцидента с момента его возникновения



Актуальные проблемы информационной безопасности

ТРЕНДЫ 2017 ГОДА

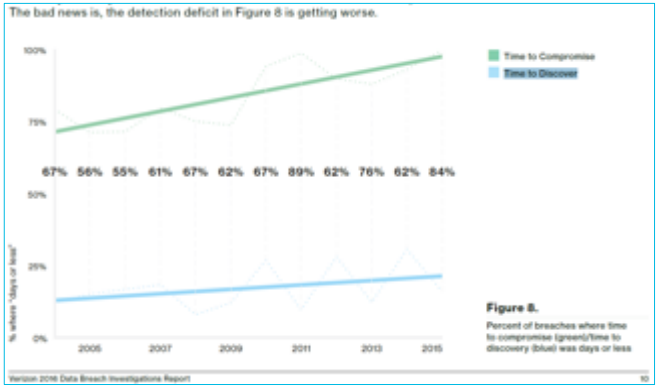
- Симметричный рост атак на клиентов банков и сами банки
- Пассивные закладки и короткие заражения (Crime-as-a-Service)
- Использование Internet of things в атаках
- Сигнатуры малоэффективны
- Поддельные сайты
- Рост времени обнаружения инцидента с момента его возникновения



Актуальные проблемы информационной безопасности

ТРЕНДЫ 2017 ГОДА

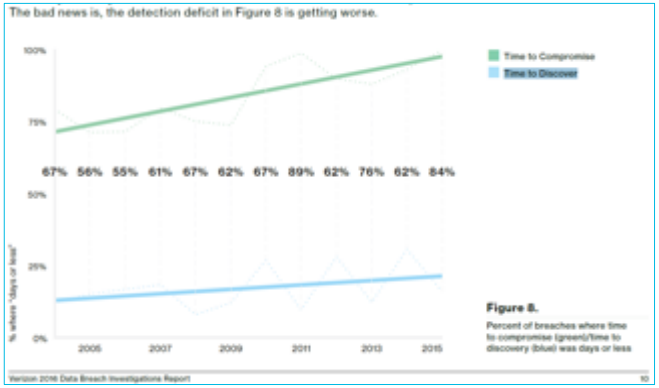
- Симметричный рост атак на клиентов банков и сами банки
- Пассивные закладки и короткие заражения (Crime-as-a-Service)
- Использование Internet of things в атаках
- Сигнатуры малоэффективны
- Поддельные сайты
- Рост времени обнаружения инцидента с момента его возникновения



Актуальные проблемы информационной безопасности

ТРЕНДЫ 2017 ГОДА

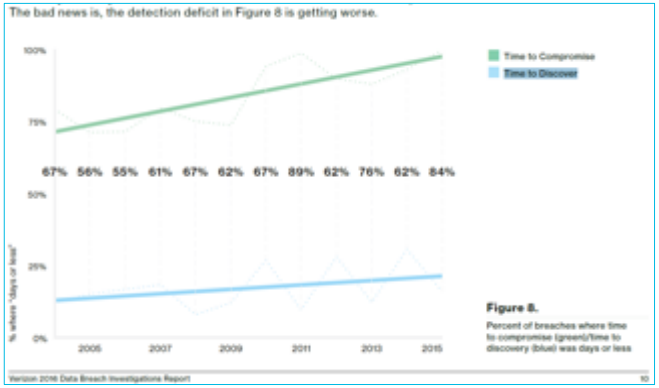
- Симметричный рост атак на клиентов банков и сами банки
- Пассивные закладки и короткие заражения (Crime-as-a-Service)
- Использование Internet of things в атаках
- Сигнатуры малоэффективны
- Поддельные сайты
- Рост времени обнаружения инцидента с момента его возникновения



Актуальные проблемы информационной безопасности

ТРЕНДЫ 2017 ГОДА

- Симметричный рост атак на клиентов банков и сами банки
- Пассивные закладки и короткие заражения (Crime-as-a-Service)
- Использование Internet of things в атаках
- Сигнатуры малоэффективны
- Поддельные сайты
- Рост времени обнаружения инцидента с момента его возникновения



Ключевые угрозы 2017. Финансовые потери

Внедрение в платежные процессы и изменение платежной информации, в том числе

- с использованием удаленного доступа внешних злоумышленников
- с использованием помощи работников внешним злоумышленникам
- внешними злоумышленниками через интеграции с партнерами и контрагентами
- легитимными пользователями

Несанкционированный доступ к контактным данным клиентов для последующего подключения к каналам обслуживания от их имени

- с использованием удаленного доступа внешних злоумышленников
- с использованием помощи работников внешним злоумышленникам
- легитимными пользователями

Удаленный доступ в инфраструктуру

- malware
- криптолокеры
- доступ к платежным системам
- непростые атаки (пассивные импланты, кратковременные заражения, вредоносы в доверенном ПО)
- атаки на банкоматы

Почему организациям нужен SOC?

Усложнение атак и постоянное развитие угроз заставляет адекватно реагировать на самые неожиданные угрозы

Реагирование на инциденты

Как должно быть в адекватных организациях

Подготовка

Инвентаризация

Вектора и сценарии атак

Контроли

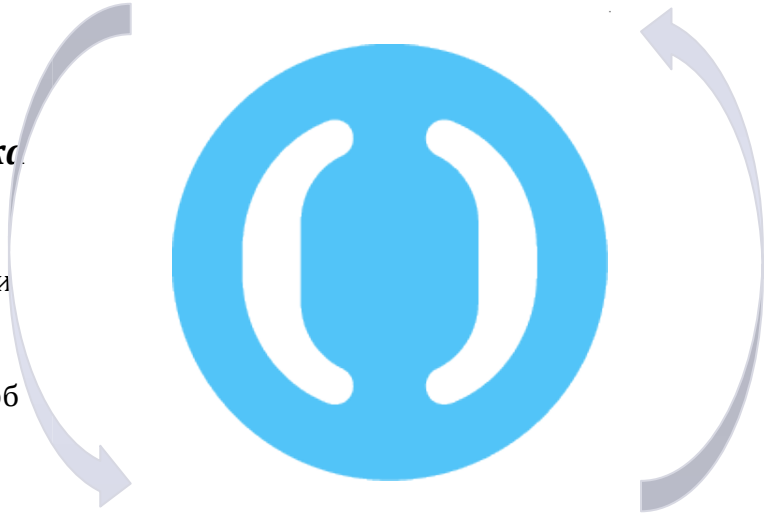
Тестирование плана реагирования

Улучшение контролей

Превентивные меры

Правила выявления и реагирования

Повышение качества аналитики



Идентификация и оценка

Распределение ролей

Разбор вектора и техник атаки

Приоритезация активностей

Трэкинг и сбор информации об атакуемых активах, потерях

Документирование

Создание отчетов

Анализ причин и несовершенств

Обучение

Сдерживание, устранение и восстановление

Принятие превентивных мер

Восстановление убытков (при их наличии)

Изоляция активов

Акцентирование мониторинга

Реагирование на инциденты

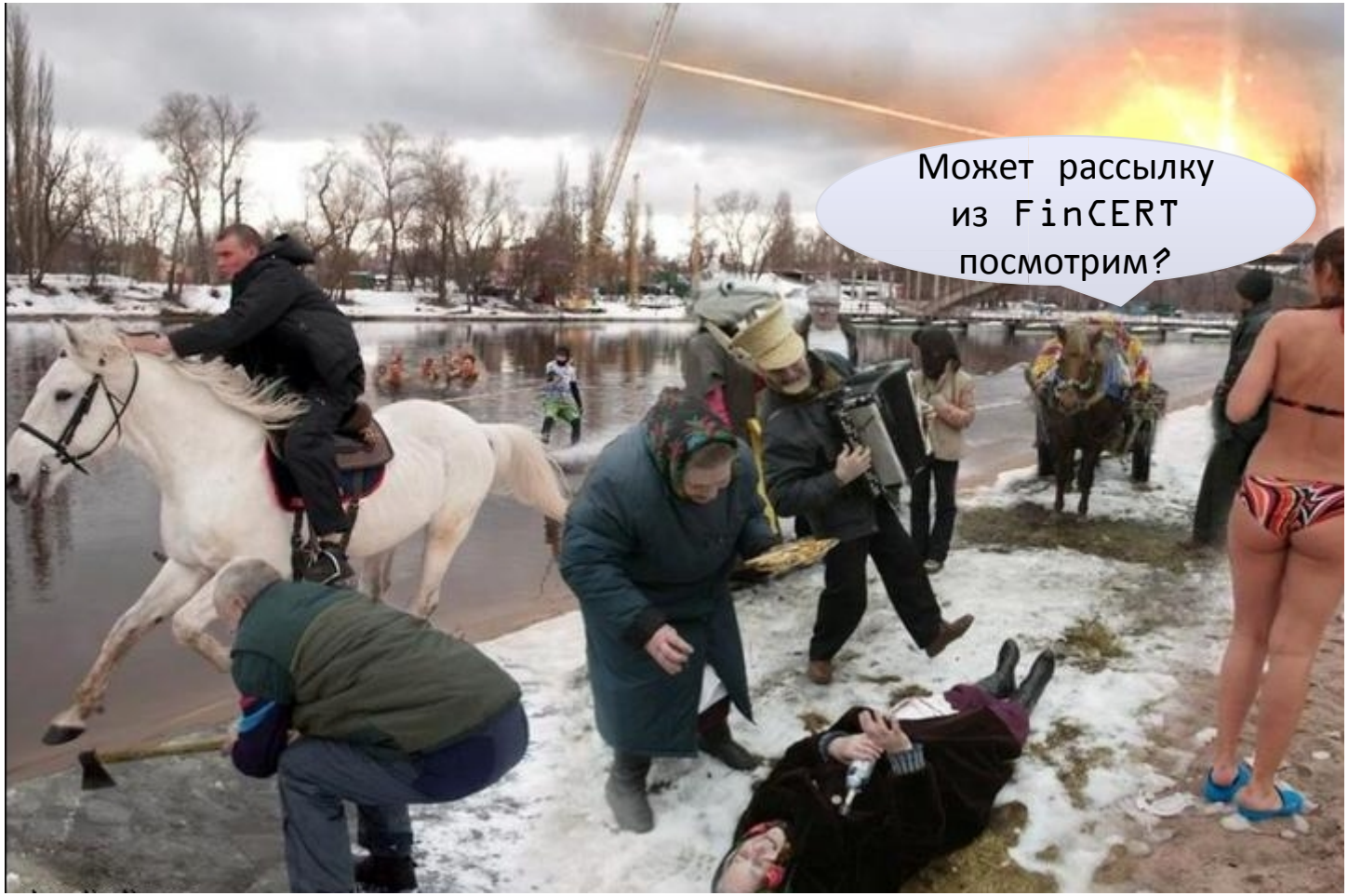
Как запланировано в НЕзрелых компаниях

Что происходит в случае инцидента?

В НЕзрелых компаниях

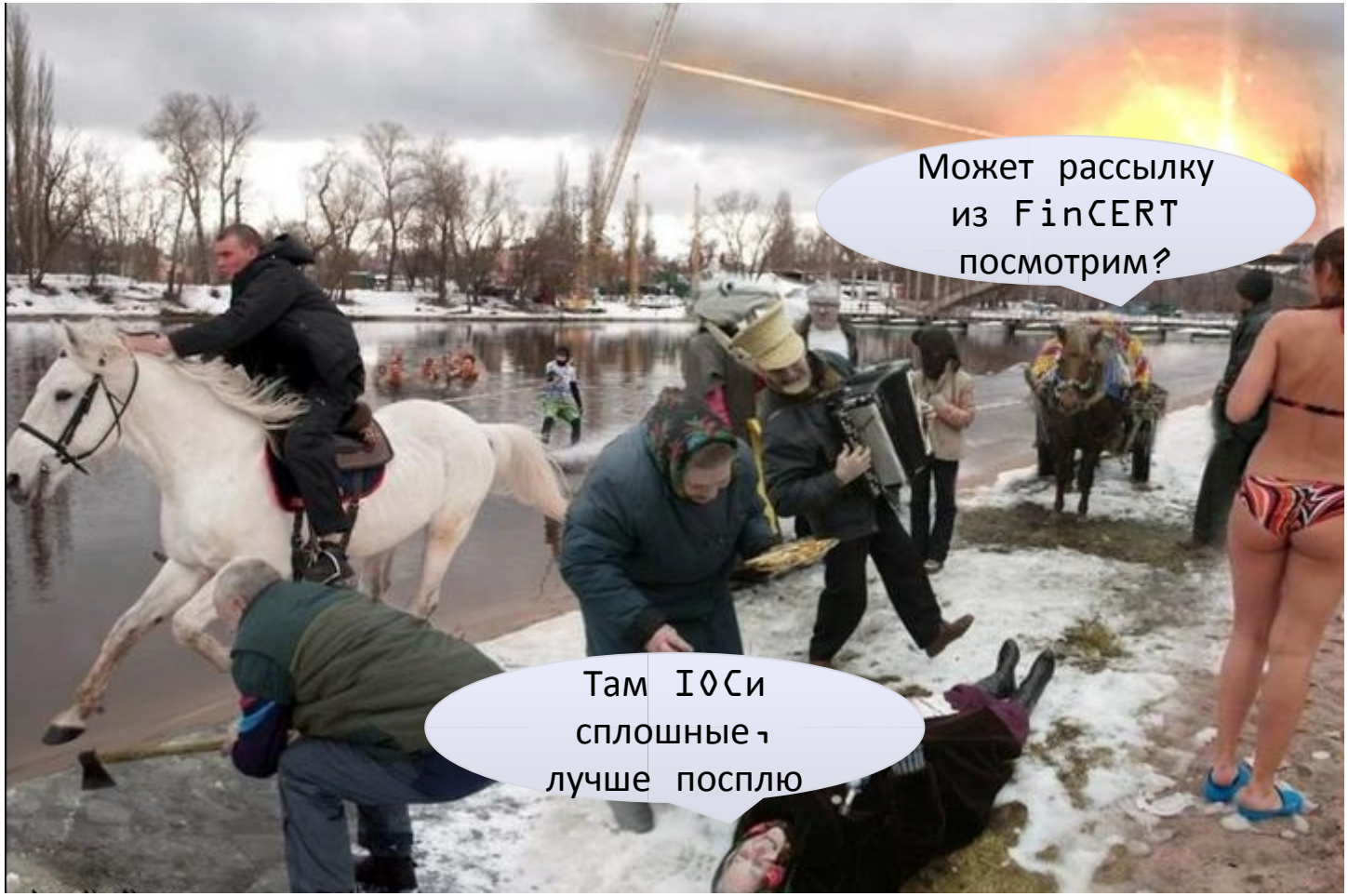
Что происходит в случае инцидента?

В НЕзрелых компаниях



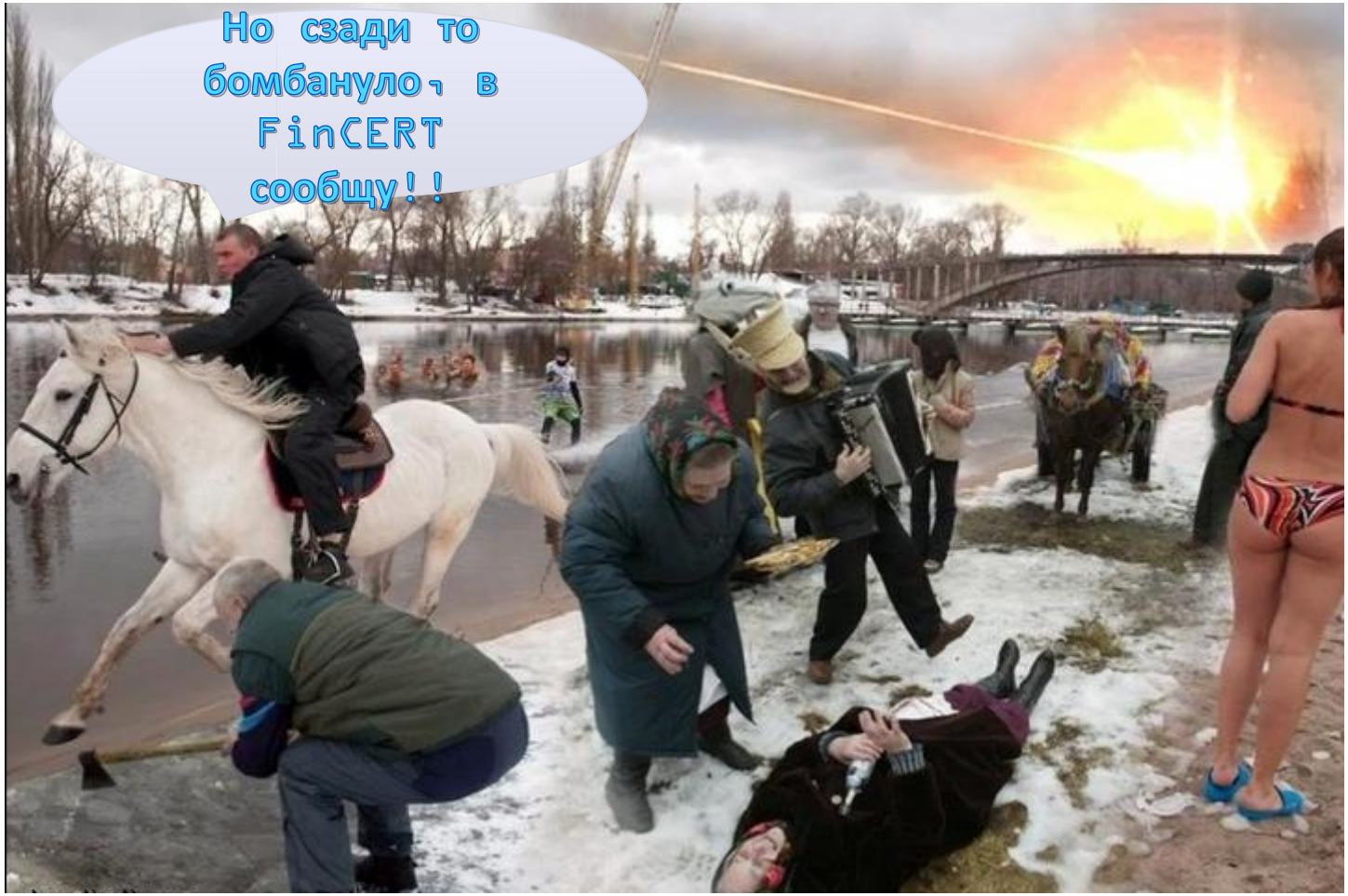
Что происходит в случае инцидента?

В НЕзрелых компаниях



Что происходит в случае инцидента?

В НЕзрелых компаниях



Сущность FinCERT

Ребята могут

Разобрать сэмпл зловреда

Сущность FinCERT

Ребята могут

Разобрать сэмпл зловреда

Получить информацию об IP C&C и сообщить банкам

Сущность FinCERT

Ребята могут

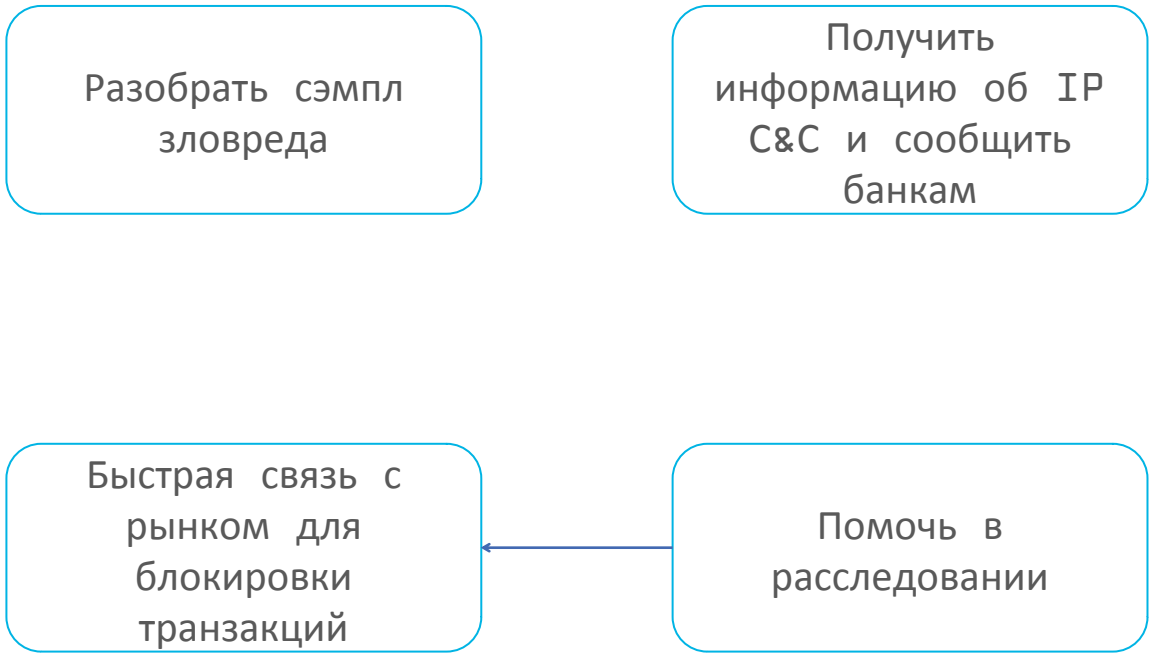
Разобрать сэмпл зловреда

Получить информацию об IP C&C и сообщить банкам

Помочь в расследовании

Сущность FinCERT

Ребята могут

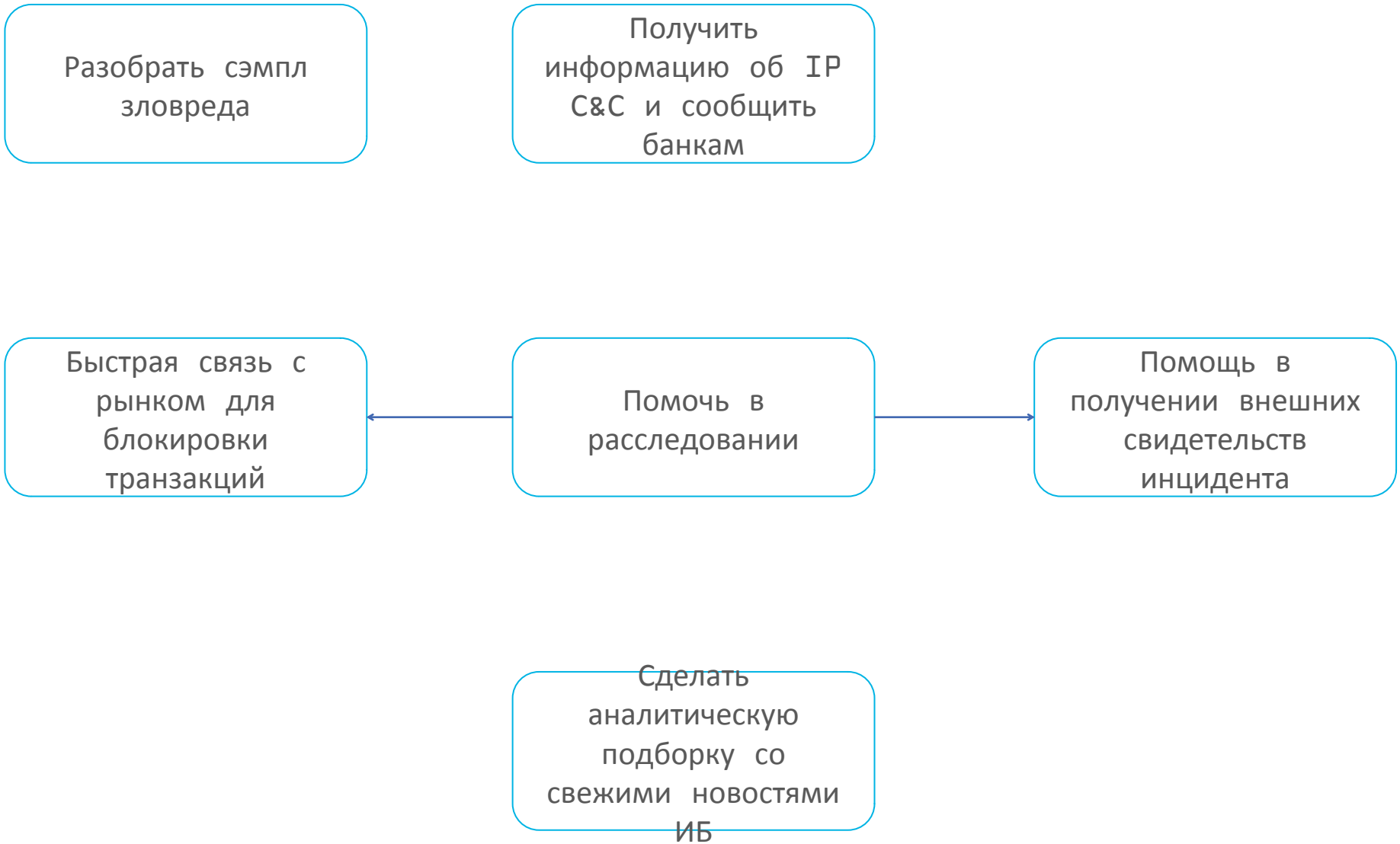


Сущность FinCERT

Ребята могут

Сущность FinCERT

Ребята могут



Сущность FinCERT

Ребята могут

Немного про паразитизм

Вместо заключения

- Надо наконец-то **заняться информационной безопасностью** и делать это очень хорошо (**не паразитировать на теле бизнеса**)
- FinCERT действительно помогает даже ребятам из пункта выше
- FinCERT - очень хороший инструмент, дополняющий SOC фидами и опциями при реагировании
- FinCERT не сделает все за банк, если банк допустил внешнюю атаку и многомиллионную кражу, но поможет в коммуникациях

Спасибо за внимание!

Касимов Вячеслав
Банк «Открытие»
Исполнительный директор по информационной безопасности

Моб.: +7 (916) 8069640
E-mail: kasimov@open.ru