

- **Вопросы и действия в текущей ситуации в сфере ИБ**
- **Обеспечение ИБ в сфере промышленности**



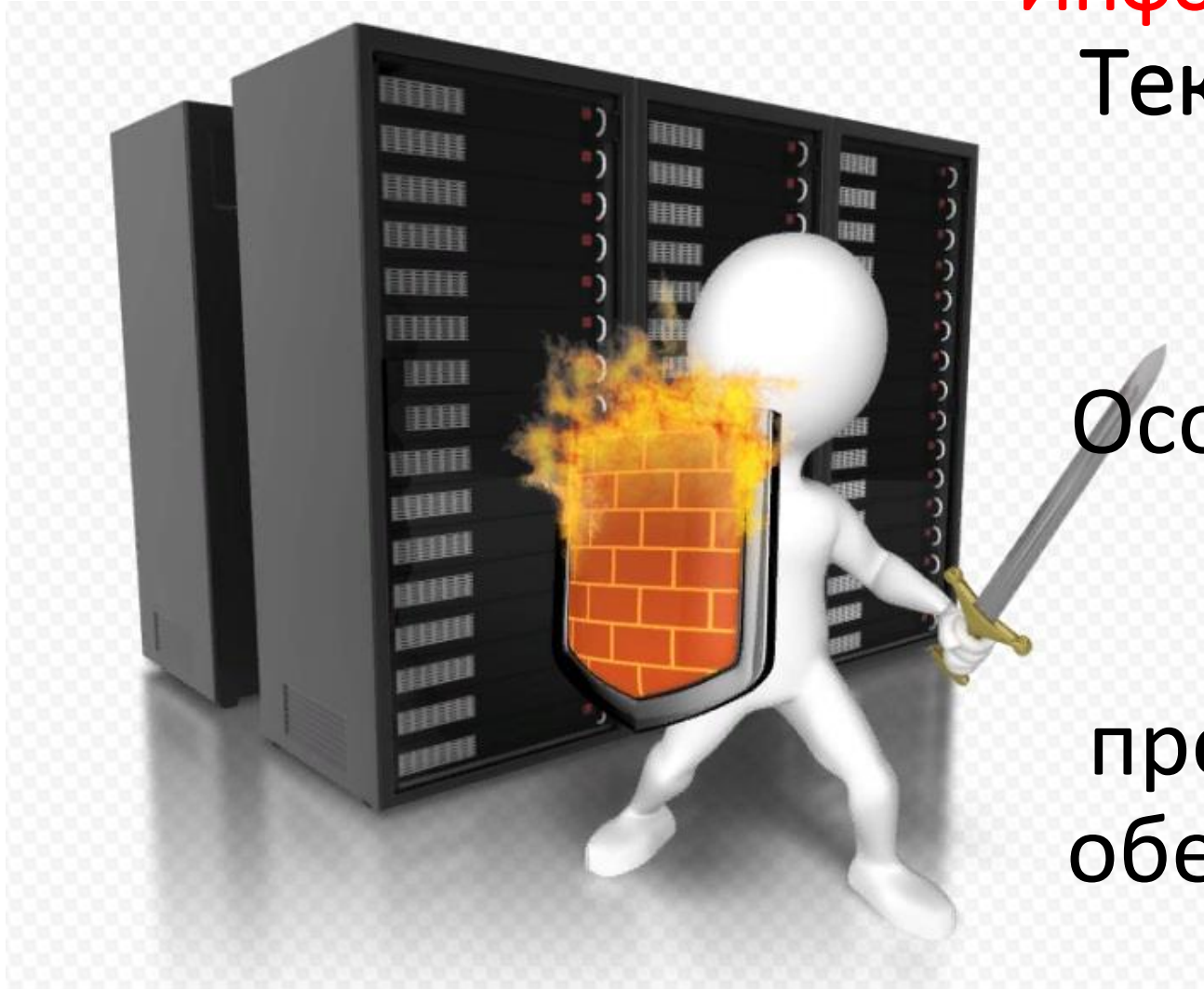
**Кузнецов Станислав Игоревич**

Руководитель подразделения ИБ АО «Завод № 9», Екатеринбург.

Главный эксперт по ЗИ АО «Астиаг» г. Сосновый Бор.

Екатеринбург

2022 г.



## Информационная безопасность.

Текущая ситуация в сфере  
обеспечения ИБ на  
производстве

Особенности практической  
коммуникации с  
менеджментом  
предприятий по вопросам  
обеспечения ИБ и ЗИ (ТЗИ).

# Управление предприятием – финансовая целесообразность и маржинальность



Что такое и где тут информационная безопасность?

# Технологические разрывы в управлении ИБ на предприятии - 1

**СЕКРЕТ ПОЛИШИНЕЛЯ (секрет на весь свет)**

**Разрыв 1, «верхний»!**

**Руководство предприятием и подразделение ИБ. Реальность!**

**ДАНО.**

- Разные цели руководства и подразделения ИБ предприятия.
- Разные основы принятия решений на коррекцию процессов.
- Пропась в мотивах финансовых трат.
- Разный уровень приоритетов, задач, ответственности за «здоровье» предприятия.

# Задача ИБ – Поймать «шпиона»!

- Оценка (примерный подсчет) ущерба от простоя процессов автоматизации информационного взаимодействия и утраты данных (оценочный уровень снижения маржинальности).
- Оценка информационных ресурсов предприятия через взаимодействие с владельцами ценных ресурсов (ноу-хау).
- Тиражирование информации о штрафных санкциях и влиянии инцидентов ИБ на деловую репутацию предприятия, (на слабо!).
- Мониторинг сети интернет на предмет актуальных инцидентов в сфере ИБ (подобных) для трансляции пользователям. «3» и «4»;
- Анализ активности пользователей для внутренней безопасности.

# Рост числа глобальных инфраструктурных инцидентов ИБ после начала СВО – ФАКТ!

## ЦЕЛИ саботажа и не исполнения договорных обязательств:

- Противодействие развитию информационной инфраструктуры России и укреплению принимаемых мер ИБ. (CISCO).
- Создание условий для возникновения элементов хаоса в управлении предприятиями (D-Dos), усложнение управления.
- Торможение планов реализации текущих программ развития и модернизации информационной инфраструктуры предприятий (Импортозамещение в «железе» и софте, внешние угрозы ИБ).
- Рост цен на привычные инструменты ИБ и удлинение сроков их развертывания и настройки в производственные цепочки (КИИ).

# Технологические разрывы в управлении ИБ на предприятии - 2

**Правда жизни.**

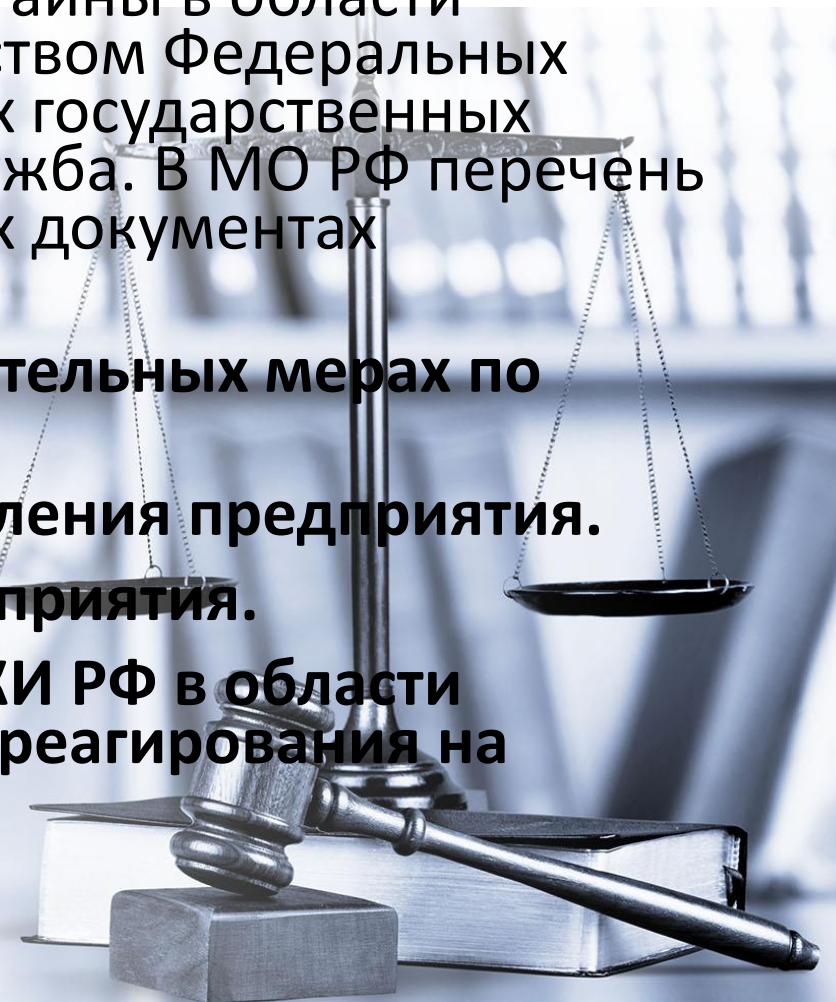
**Разрыв 2, «нижний»!**

**ДАНО:**

1. Уровень текущих действий сотрудника ИБ по реагированию на инциденты и управлению рисками «на земле» - горизонтальный!
2. ИБ вмешивается в технологические процессы производства и мешает привычной «свободе» действий сотрудников.
3. Попытки «войти в положение!», «понять и простить!», «ОНО само!», «Я ничего не делала, только на кнопку нажала!».

# Модернизация законодательства в помощь

- 172-ФЗ от 11.06.21 внесены изменения в 61-ФЗ «Об обороне» - установление нового вида тайны – служебной тайны в области обороны. Основание отнесения – утв. Руководством Федеральных органов исполнительной власти и федеральных государственных органов, в которых предусмотрена военная служба. В МО РФ перечень утвержден приказом № 22 от 28.02.22. На таких документах проставляется метка «ДСП».
- **Указ Президента от 01.5.22 № 250 «О дополнительных мерах по обеспечению ИБ РФ».**
  - + подразделение ИБ в штатной структуре управления предприятия.
  - + беспрепятственный доступ ФСБ на такие предприятия.
  - + взаимодействие в переходный период с НКЦКИ РФ в области обнаружения, предупреждения, ликвидации и реагирования на инциденты ИБ.





# Шанс решения части проблем ИБ – взаимопонимание между...!

## ВЫВОД.

- Разработчик продуктовых линеек инструментов ИБ может помочь, если будет думать о стратегии развертывания его продукта на предприятии.
- Развитие СОИБ не начинается с крупных сумм на ИБ, «Аппетит приходит во время еды!».
- Дайте ИБ поймать шпиона и подумать шефу, что с этим делать!!
- Результаты работы инструментов ИБ, «от разработчика» должны быть максимально адаптированы под «земные» задачи специалиста ИБ, итак:
  - **Формализованные шаблоны регистрации инцидента в почту.**
  - **Настраиваемые перечни требований пунктов нормативных документов предприятия.**
  - **Копии направленных виновникам инцидентов документов дублируются ответственным руководителям.**

# ИБ производственной сферы

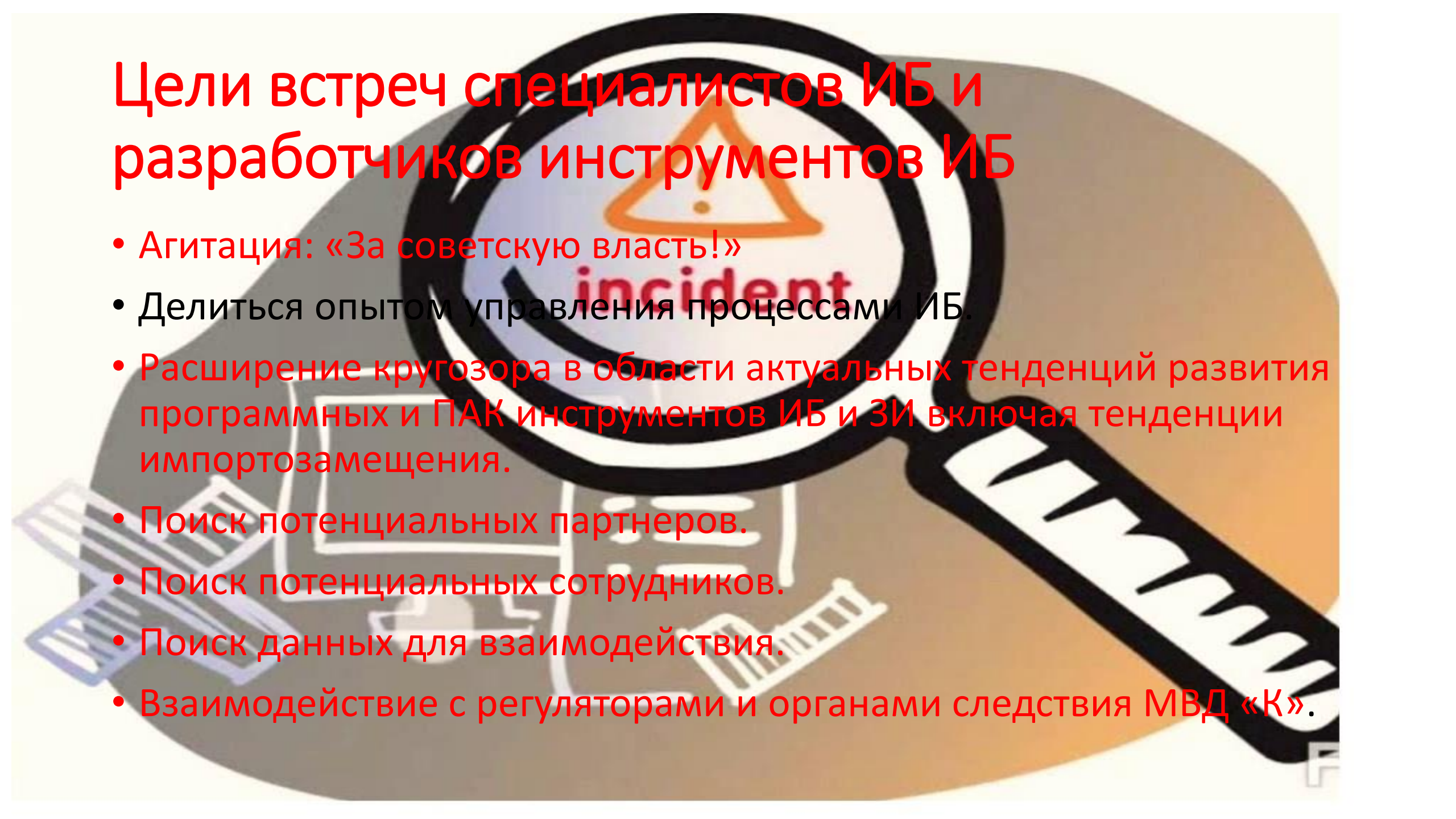
- <https://www.securitylab.ru/news/529942.php>
- <https://rt-solar.ru/events/news/2736/>
- Россия, в октябре 2020 года злоумышленникам с помощью вымогательского ПО удалось взять под управление предприятие в Рязани Steelcase, относящееся к ЗОКТИИ. Примечательным здесь стал финал: виновника допущенной ошибки нашли внутри предприятия и наказали сотрудника согласно КоАП.
- Самое важное в работе современного специалиста по безопасности – суметь обнаружить угрозу инцидента до его наступления. Не получится защититься от всего сразу, потому важно обращать внимания на индикаторы, с высокой долей вероятности сигнализирующие о проблемах в ИБ. Если говорить о мониторинге промышленной сети, то к таким можно отнести:
  - ошибки политики разграничения доступа к ресурсам и процессам;
  - появление новых неучтённых устройств – ретрансляторов информативного сигнала, потребителей;
  - появление нетипичного трафика и возникновение аномалий;
  - непроизводственная активность на подключённых в сеть устройствах.

Всё это может привести к опасным последствиям, как:

- заражению устройств и захвату управления, вымогательству (шифровальщики), воздействию ИТР;
- нарушению технологических процессов, сбои оборудования, брак, поломки и неисправности;
- несанкционированной передаче данных вовне, утечки по ПЭМИН;
- проникновению в другие сегменты сети, нарушение ПРД, расширение полномочий, привилегии.

Как уменьшить опасности – «подписать» на сотрудничество максимум пользователей сети любыми методами!

# Цели встреч специалистов ИБ и разработчиков инструментов ИБ

The background of the slide features a stylized illustration. A large magnifying glass is positioned over a warning sign that consists of a triangle with an exclamation mark inside. Below the triangle, the word "incident" is written in a red, lowercase font. The magnifying glass has a black handle with white text that is partially visible. In the lower-left corner, there is a faint illustration of a computer keyboard.

- Агитация: «За советскую власть!»
- Делиться опытом управления процессами ИБ.
- Расширение кругозора в области актуальных тенденций развития программных и ПАК инструментов ИБ и ЗИ включая тенденции импортозамещения.
- Поиск потенциальных партнеров.
- Поиск потенциальных сотрудников.
- Поиск данных для взаимодействия.
- Взаимодействие с регуляторами и органами следствия МВД «К».

Вопросы можно лично!

- Готов к дискуссии...

**Спасибо за внимание!**

