

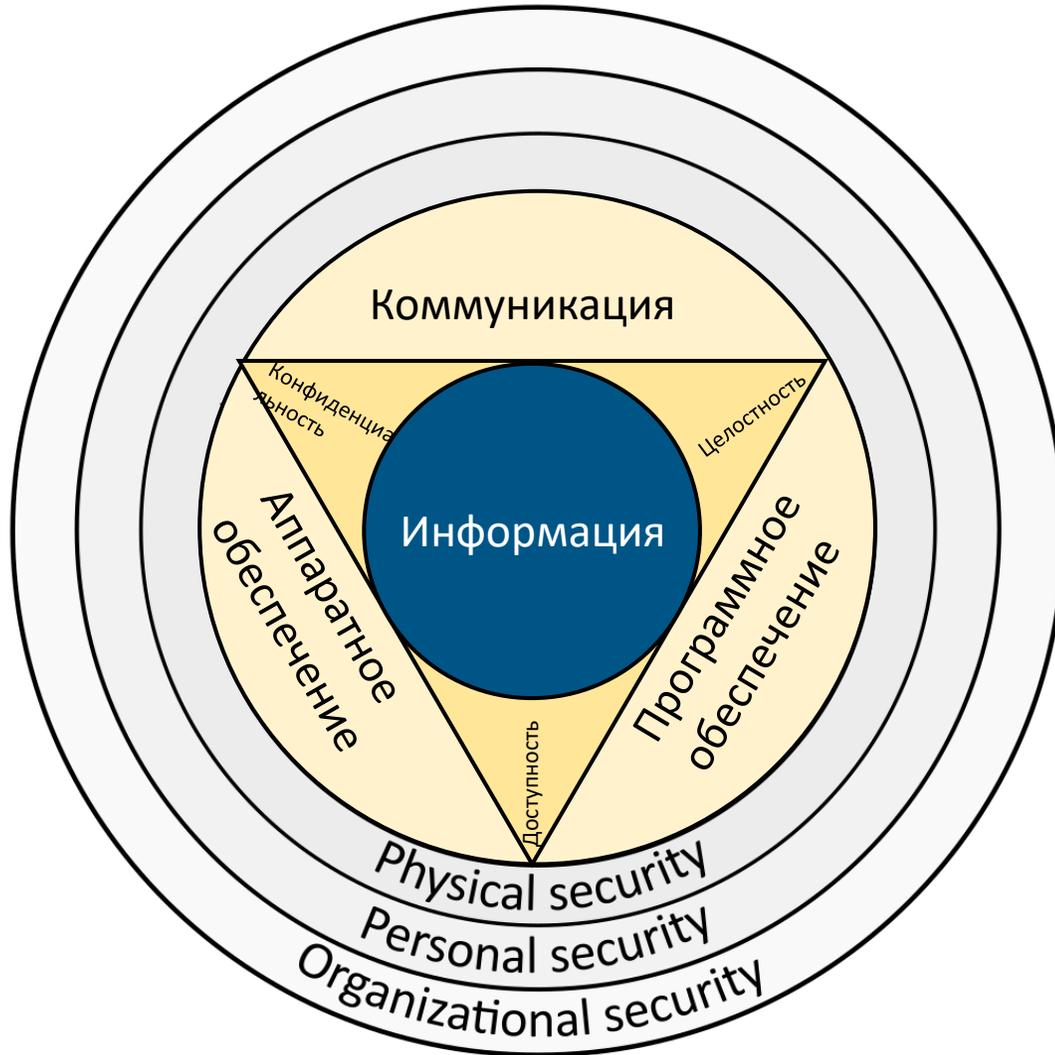


ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ «РОЛЬ CISO ДЛЯ БИЗНЕСА»

ДАВИД МАМЕДОВ



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



Информационная безопасность

Информационные системы состоят из трех основных частей: **аппаратного обеспечения, программного обеспечения и средств связи**, для определения и применения отраслевых стандартов информационной безопасности в качестве механизмов защиты и предотвращения на трех уровнях: **физическом, личном и организационном**. По сути, процедуры или политики внедряются, чтобы ознакомить администраторов, пользователей и операторов с тем, как использовать продукты для обеспечения информационной безопасности в организациях.

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (СУИБ)

- **СУИБ** — это часть общей системы управления организации, основанной на оценке бизнес рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности.

-
- **Первый принцип** заключается в том, что система управления информационной безопасностью (СУИБ) является неотъемлемой частью общей системы менеджмента организации. CISO, таким образом, выступает в роли менеджера по процессам информационной безопасности.
 - **Второй принцип** подчеркивает зависимость уровня и области применения информационной безопасности от контекста организации, в которой создается СУИБ.

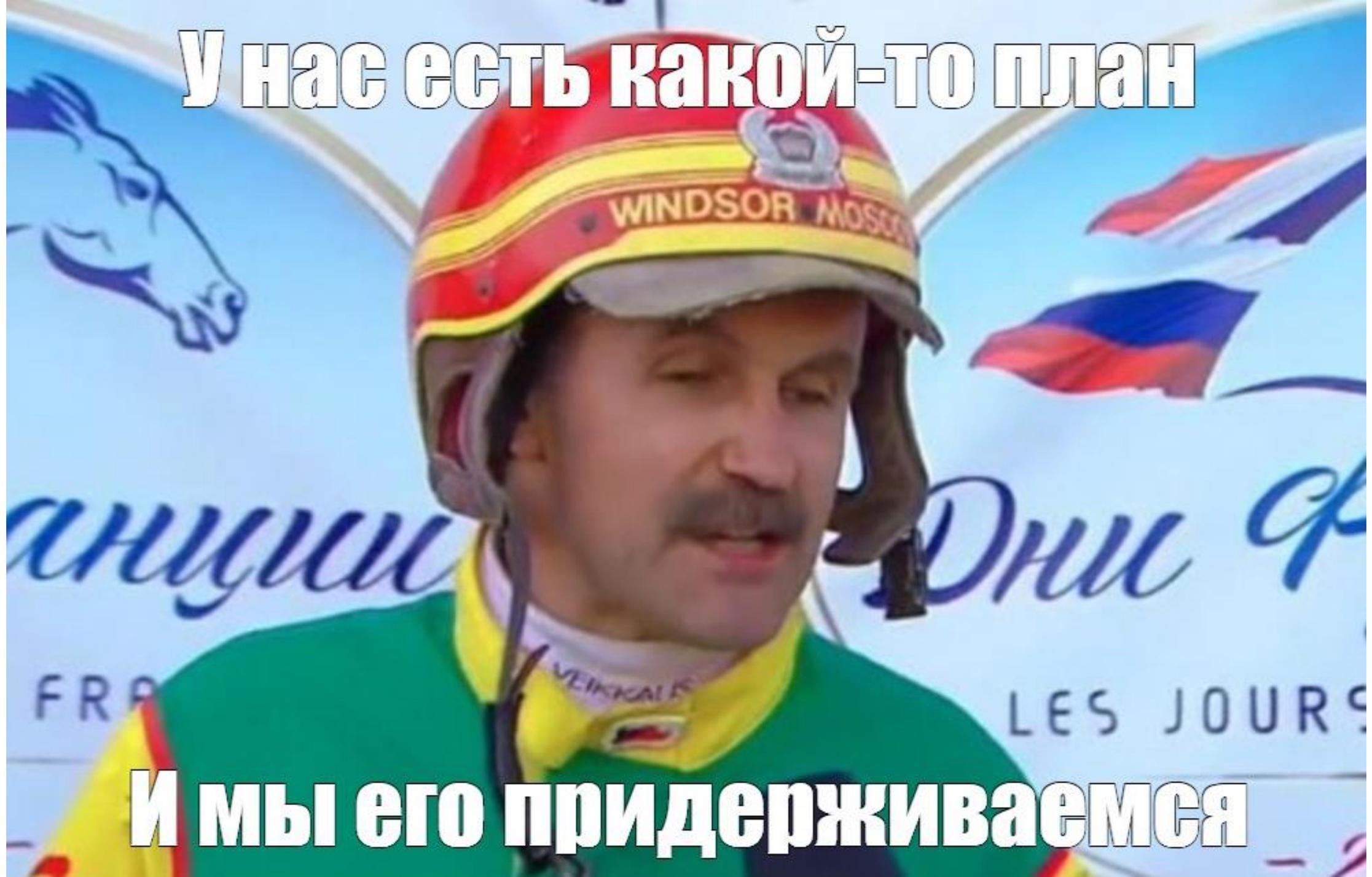
- **Основные понятия**

- **Конфиденциальность** — обеспечение доступа к информации только авторизованным пользователям;
- **Целостность** — Обеспечение точности и полноты информации и методов ее обработки;
- **Доступность** — предоставление доступа к информации и связанным с ней активам авторизованным пользователям по мере необходимости;



- COBIT
 - NIST SP 800-53
 - NIST SP 800-171
 - NIST Cybersecurity Framework
 - NIST SP 1800 Series
 - ISO 27000 Series
 - CIS Controls
 - HITRUST CSF
 - GDPR
 - COSO

У нас есть какой-то план

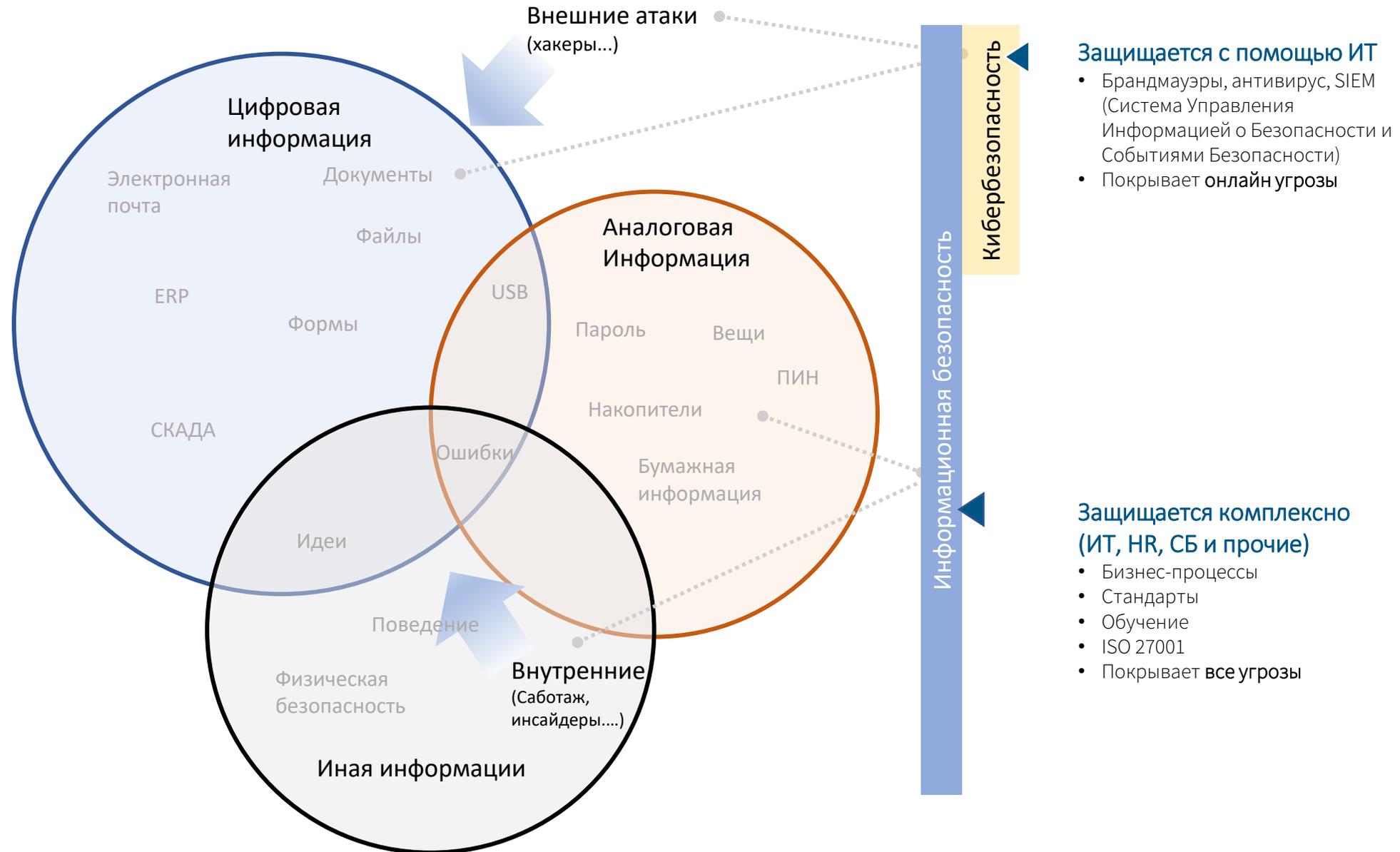


И мы его придерживаемся

ВЕЛИКОЛЕПНЫЙ ПЛАН, ЕСЛИ Я ВСЕ ПРАВИЛЬНО ПОНЯЛ!



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КИБЕРБЕЗОПАСНОСТЬ



Я ВСЕ
СПЛАНИРОВАЛ!

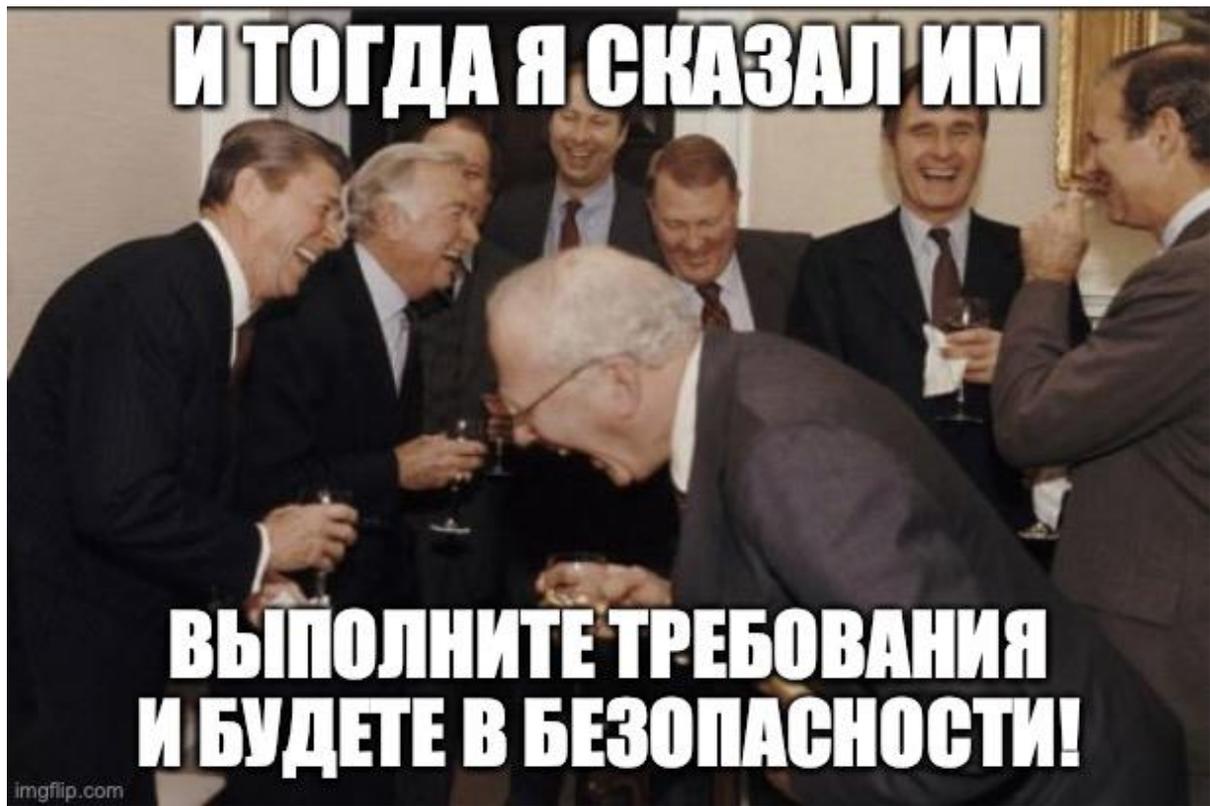
НУЖНЫ
ДЕНЬГИ!

Я НЕ ЧАСТО ДУМАЮ О КИБЕРБЕЗОПАСНОСТИ

НО КОГДА ДУМАЮ, КАК ПРАВИЛО, УЖЕ ПОЗДНО



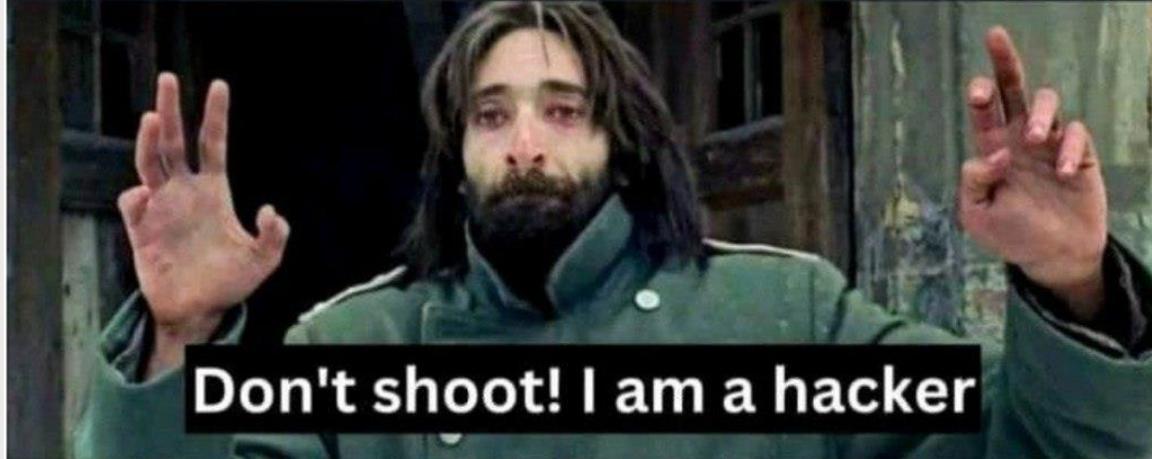
ТРЕБОВАНИЯ РЕГУЛЯТОРОВ И АУДИТОРОВ КАК ИНСТРУМЕНТ CISO



РЕГУЛЯТОР



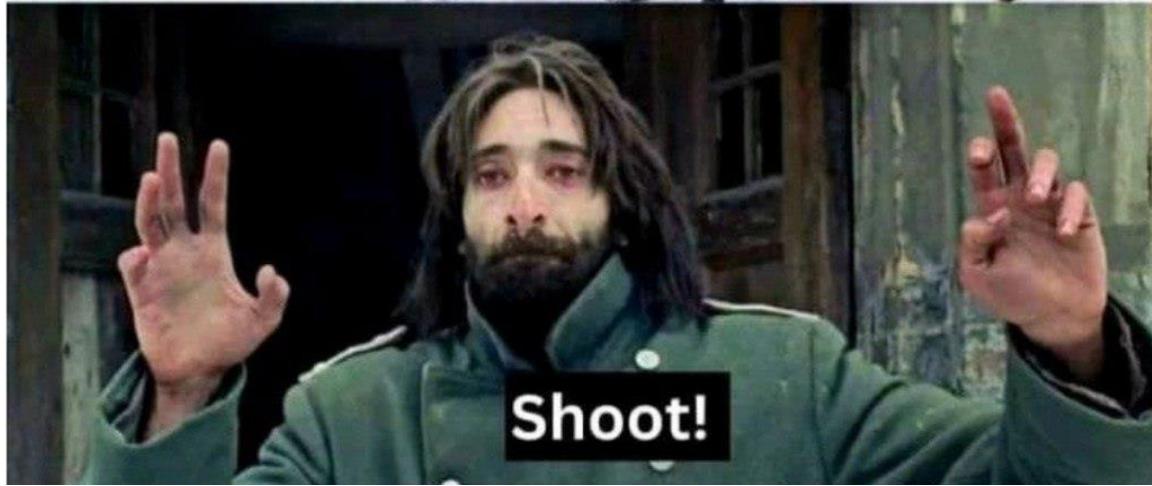
АУДИТОР



Don't shoot! I am a hacker



Can you fix my printer?



Shoot!

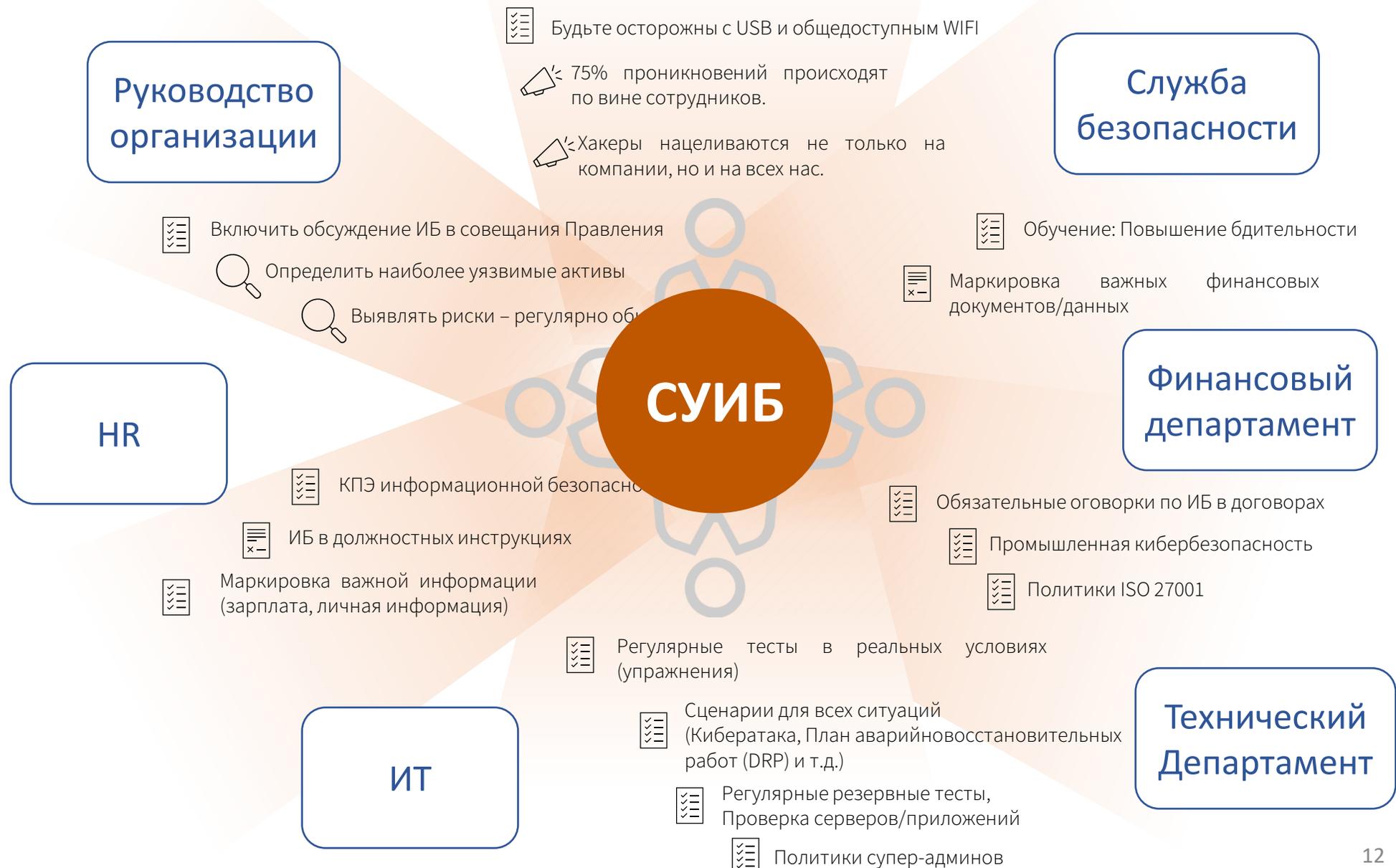
**БОЛЬ,
ТОРГ,
ПРИНЯТИЕ**

ИСТОКИ ИБ



Архивные кадры.

КОРПОРАТИВНАЯ КУЛЬТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ПРОЕКТНОЕ ПОСТРОЕНИЕ ИБ И СЗИ



PDCA КАРУСЕЛЬ





РЕАЛЬНАЯ РДСА КАРУСЕЛЬ



Я РАБОТАЮ CISO И В ЭТОМ НЕТ НИЧЕГО СЛОЖНОГО. СТАНИСЛАВ 26 ЛЕТ.

АВАРИЙНЫЙ ПЛАН (DISASTER RECOVERY PLAN)

DRP — это штука, которая в идеале никогда не понадобится. Но если вдруг мигрирующие в брачный период бобры перегрызут магистральное оптоволокно или джуниор-админ дропнет продуктивную базу, вы точно хотите быть уверены, что у вас будет заранее составленный план, что с этим всем безобразием делать.





РОЛЬ CISO ДЛЯ БИЗНЕСА

THANK YOU FOR YOUR ATTENTION!

ANY QUESTIONS?

David Mamedov
David.Mamedov@Kazminerals.com