ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

«РОЛЬ CISO ДЛЯ БИЗНЕСА»

ДАВИД
МАМЕДОВ

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;

ISO/IEC (ИСО/МЭК) 27001

- ISO/IEC 27001 — это международный стандарт управления информационной безопасностью.
- В нем подробно описаны требования к созданию, внедрению, обслуживанию и постоянному совершенствованию системы управления информационной безопасностью (СУИБ), цель которой — помочь организациям повысить безопасность своих информационных активов.

С 2005 года

Постоянный пересмотр -> упрощение

ISO/IEC 27001 требует, чтобы руководство:

- Систематически изучало **риски информационной безопасности** организации с учетом угроз, уязвимостей и воздействий;
- Разрабатывало и внедряло понятный и всеобъемлющий набор **средств контроля информационной безопасности** и/или других форм регулирования рисков (таких как исключение рисков или передача рисков) для устранения рисков, которые считаются неприемлемыми; а также
- Внедрило всеобъемлющий **процесс управления**, с целью обеспечения удовлетворения постоянно растущей потребности в управлении информационной безопасностью в организации на постоянной основе.

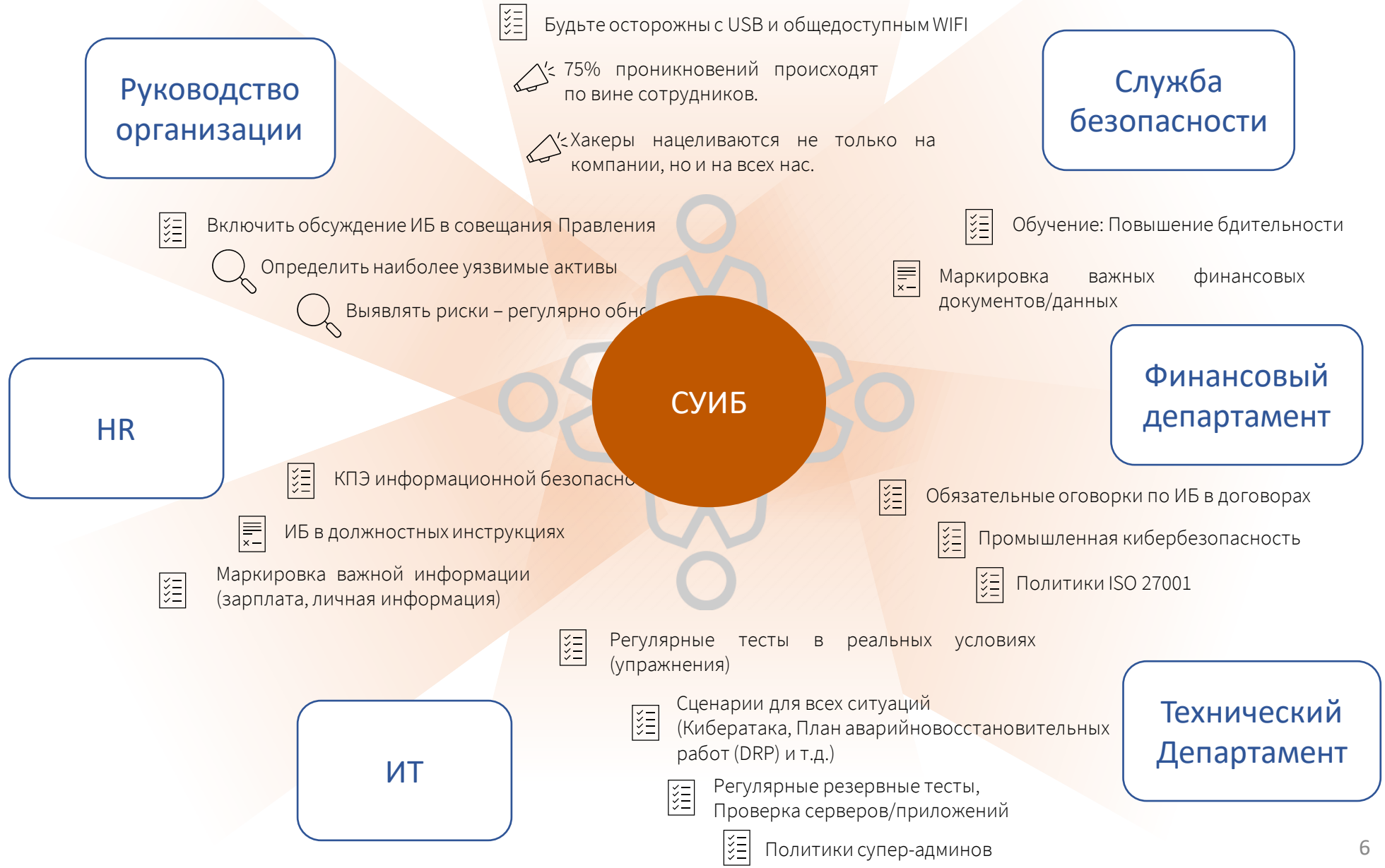
Наши ключевые принципы

- **Простота и достаточность** – минимум информации, четкая структура, самое главное
- **Начинать с самого существенного** — быстрые победы благодаря внедрению важнейшего в самом начале и дальнейшему совершенствованию по мере необходимости
- **Не нужна сертификация** - основная цель получить рабочий инструмент (при необходимости – возможность пройти сертификацию, тем самым повысив стоимость компании).

ПИРАМИДА ПОСТРОЕНИЯ СУИБ

Может быть в этом году мы попробуем
иную стратегию кибербезопасности?

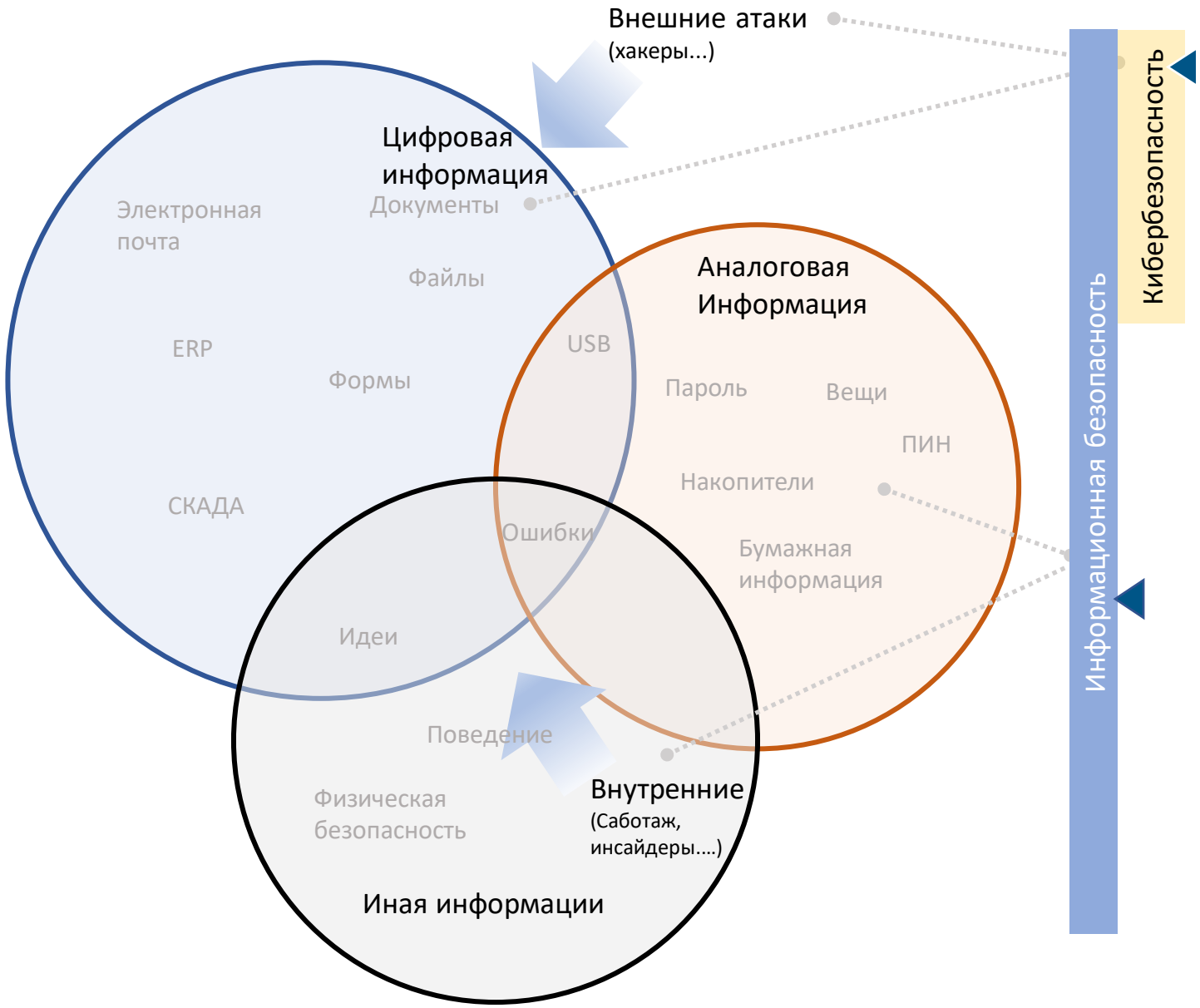
КОРПОРАТИВНАЯ КУЛЬТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



МОИ ПОЗДРАВЛЕНИЯ! ВЫ ПРОШЛИ ИБ!!!

БОЛЬ,
ТОРГ,
ПРИНЯТИЕ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КИБЕРБЕЗОПАСНОСТЬ



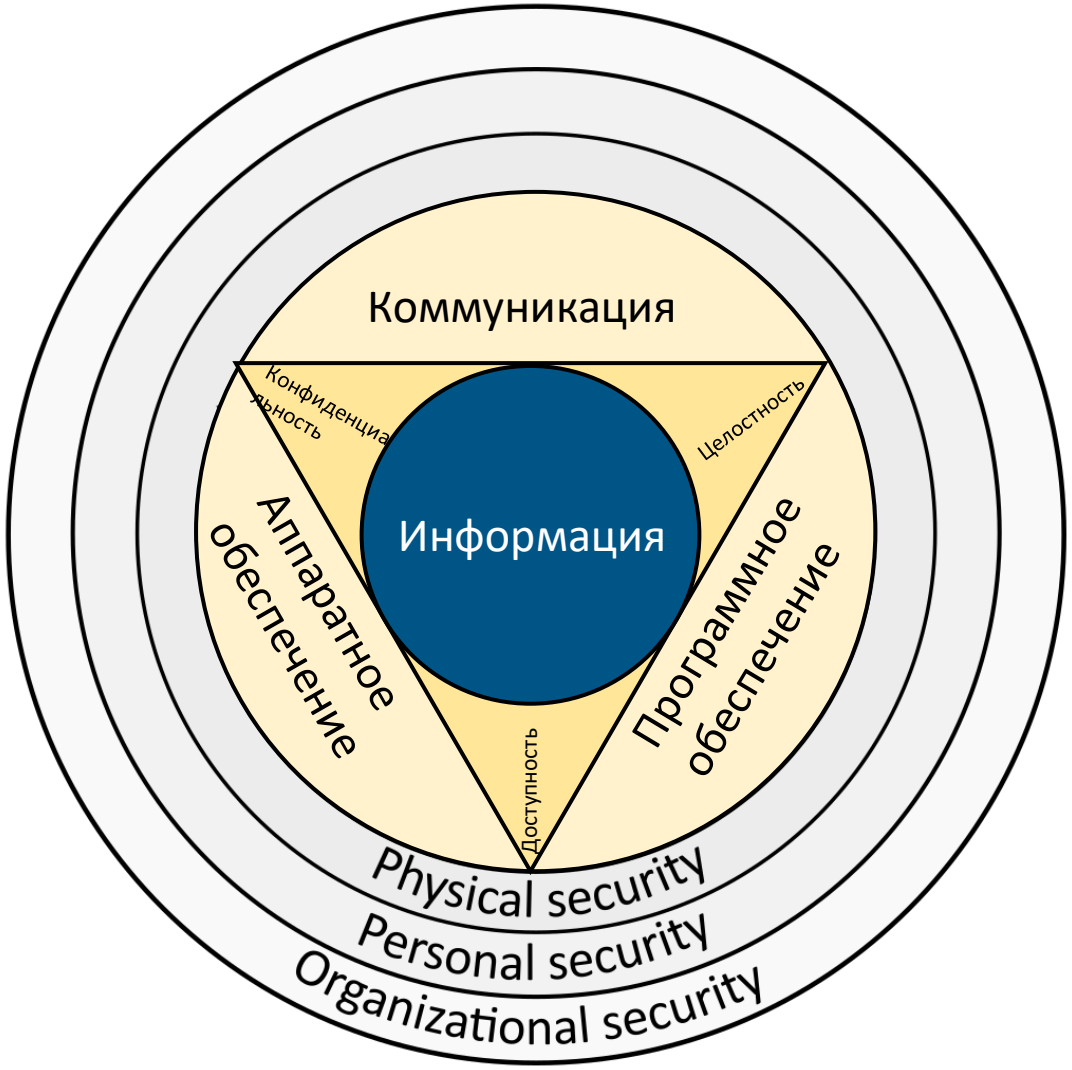
Защищается с помощью ИТ

- Брандмауэры, антивирус, SIEM (Система Управления Информацией о Безопасности и Событиями Безопасности)
- Покрывает **онлайн угрозы**

Защищается комплексно (ИТ, HR, СБ и прочие)

- Бизнес-процессы
- Стандарты
- Обучение
- ISO 27001
- Покрывает **все угрозы**

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.

INFORMATION SECURITY MANAGEMENT SYSTEM

A little bit of humor

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