Специалист по информационной безопасности сегодня и завтра:

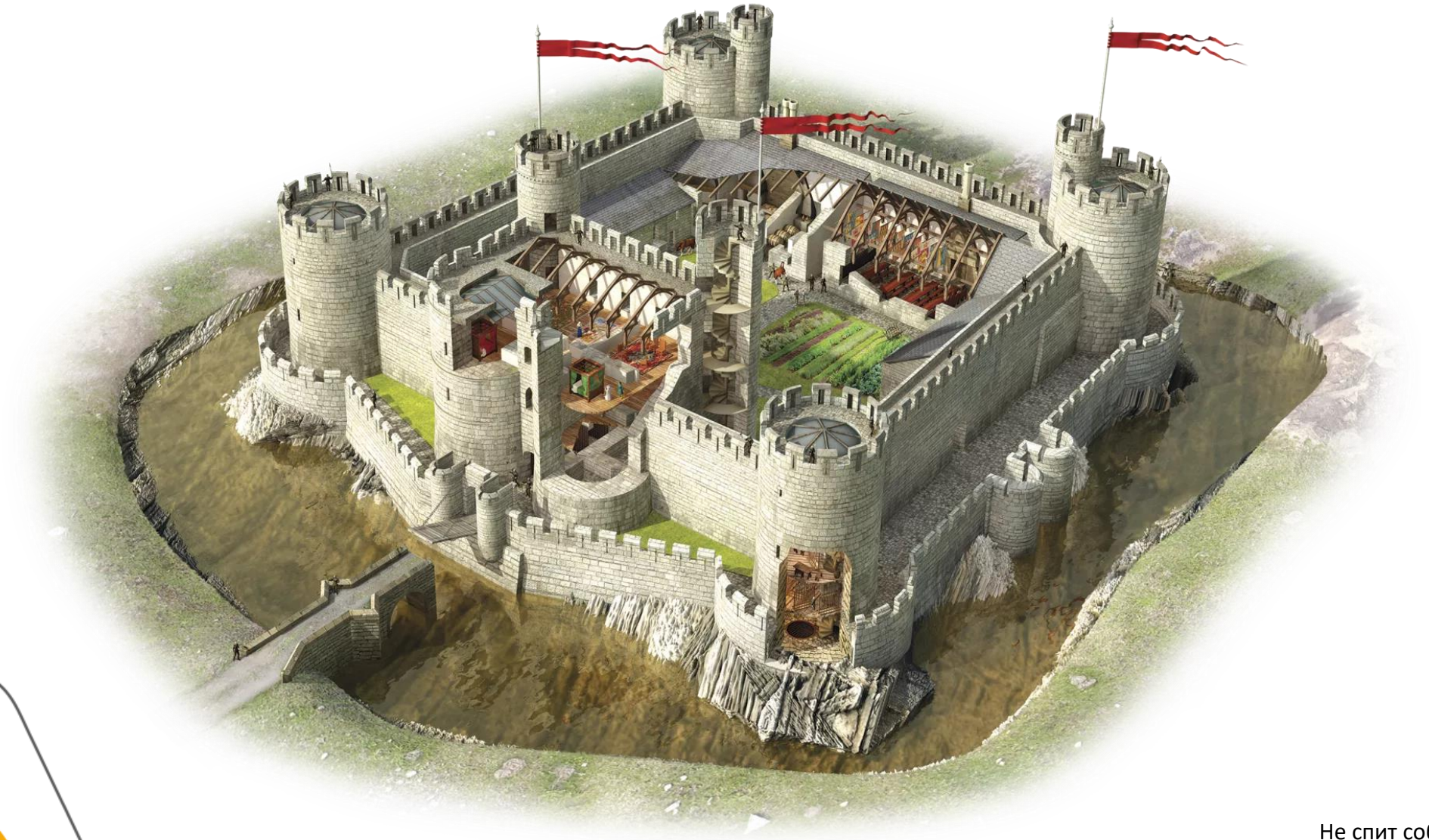
актуальные потребности рынка

УЦСБ

Николай Домуховский

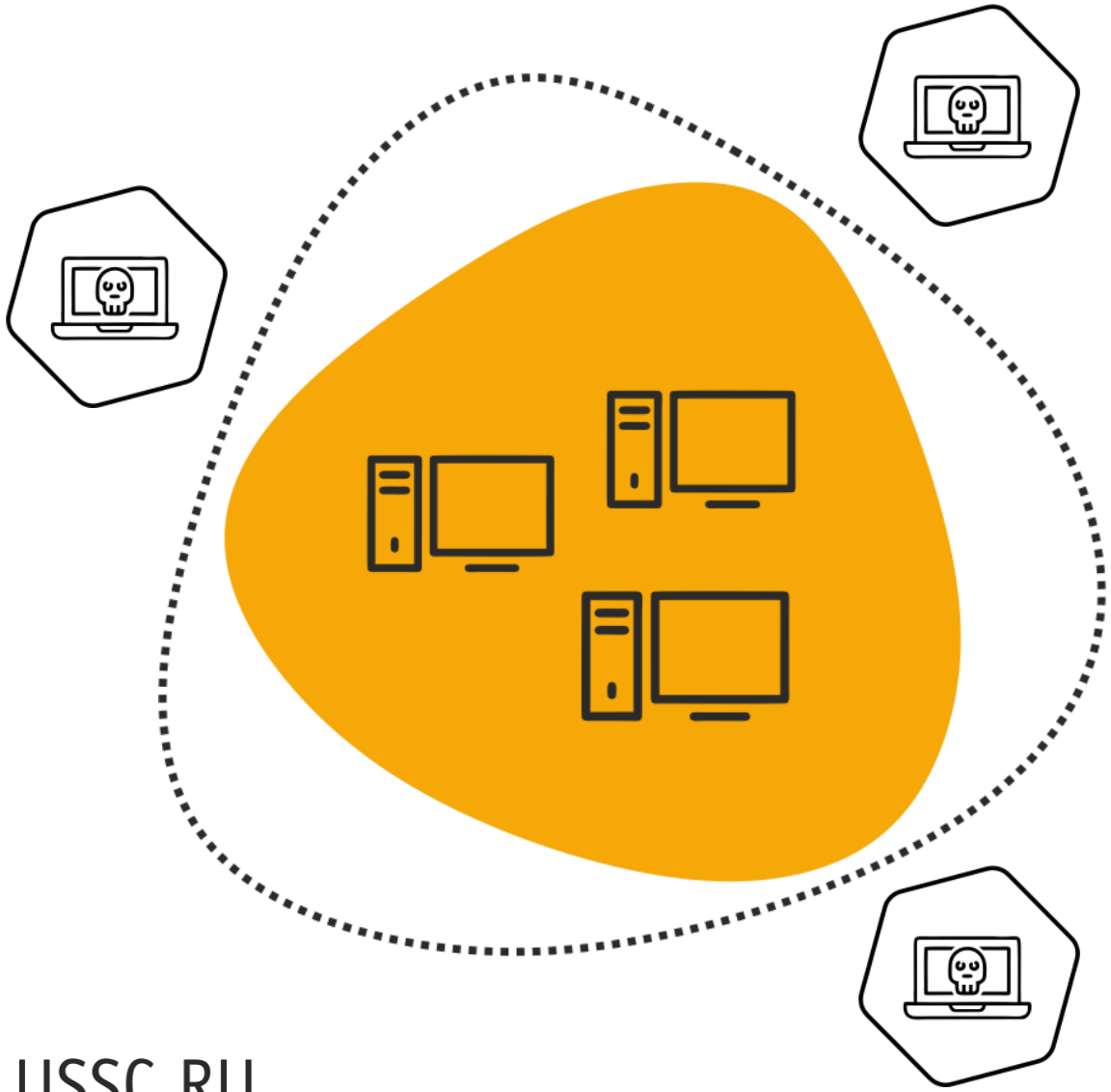
Заместитель
генерального директора
по научно-технической работе

Прошлое



Не спит собака, дачу охраняет,
И я не сплю – собаку стерегу.
М. Ножкин

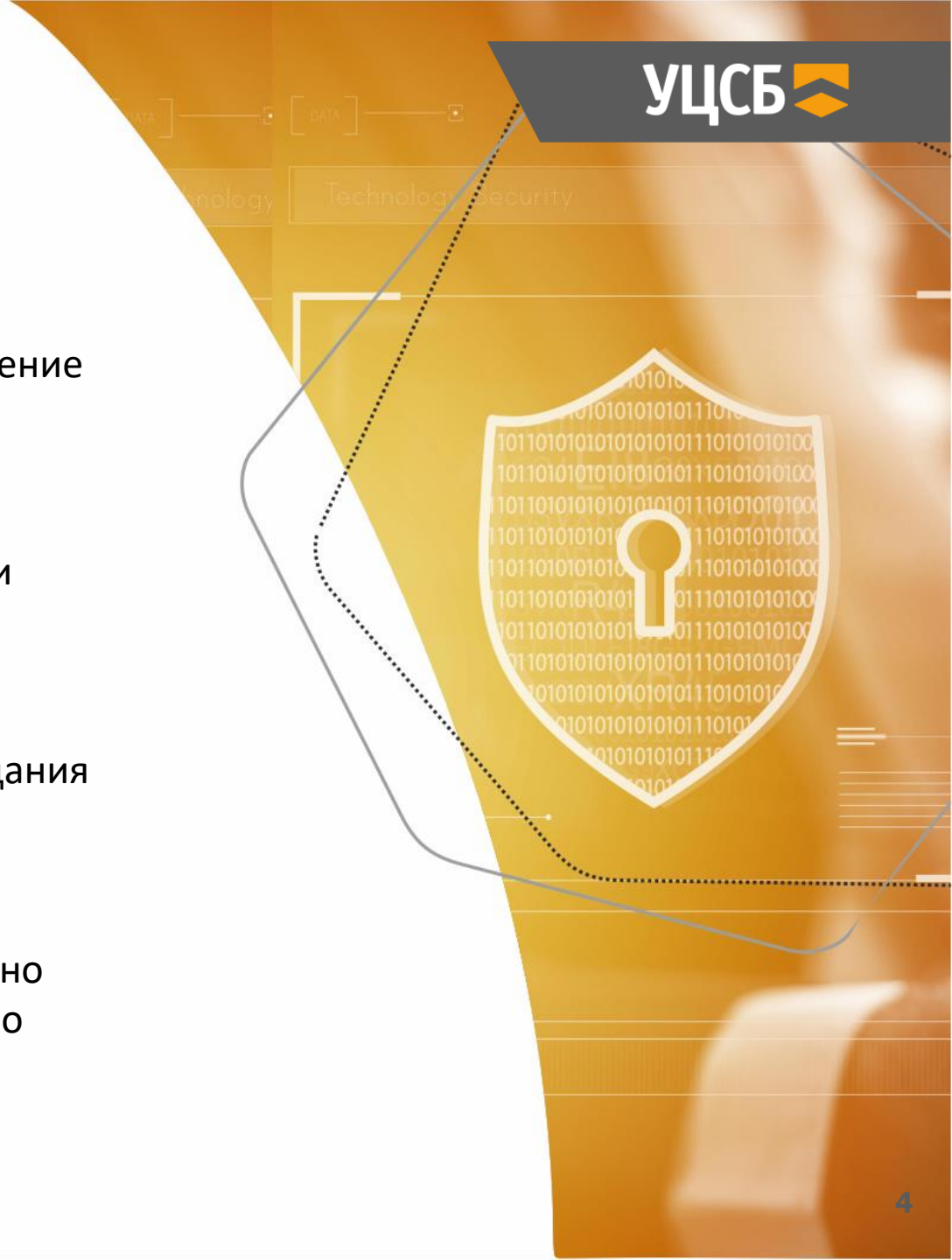
Модель «Бастион»



- Информационные системы небольшие и имеют четкий периметр
- Внутри периметра – друзья
- За периметром – враги
- Основное – периметральная защита
- Внутри – жесткое разграничение доступа

Парадигма ИБ эпохи «Бастионов»

- Абсолютный детерминизм всех процессов в системе – построение невзламываемой системы (unbreakable)
- Можно явно разделить все процессы на легитимные и нелегитимные
- Задача обеспечения ИБ решается в момент создания системы
- Требования и методы обеспечения ИБ можно унифицировать и использовать многократно



Требуемые знания и навыки специалиста по ИБ

Прикладные знания

- Механизмы безопасности встроенного ПО и ОС
- Наложенные СрЗИ от НСД
- Аттестация АС
- Формальные требования ИБ
- Сетевые технологии
- Сетевые ОС

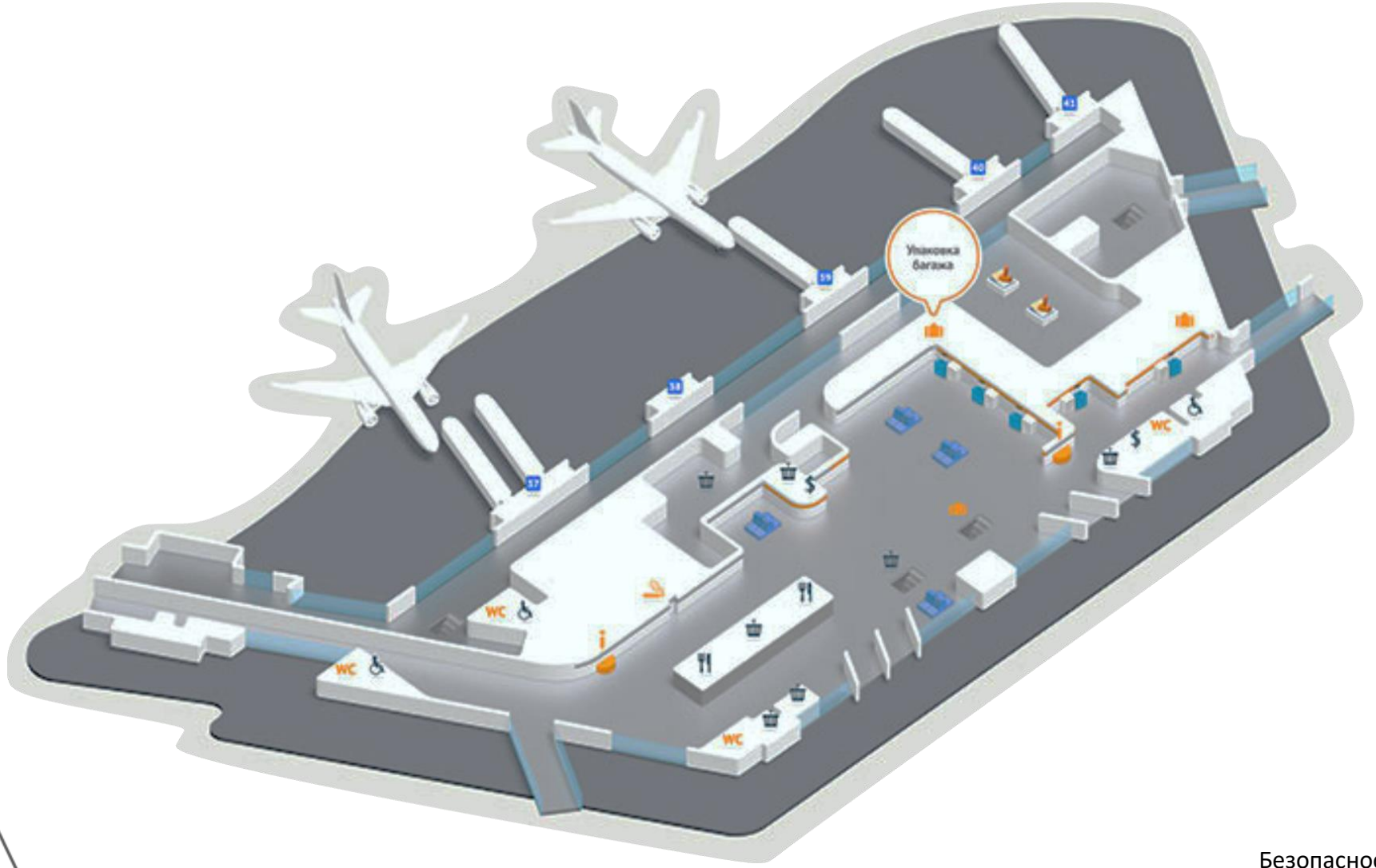
Фундаментальные знания

- Формальные модели управления доступом
- Политика ИБ
- Порядок создания АС в ЗИ
- Монитор безопасности
- Принципы пакетной передачи данных
- Свойства безопасности информации

Но всё же мы полагаем, что знание и понимание относятся больше к искусству, чем к опыту, и считаем владеющих каким-то искусством более мудрыми, чем имеющих опыт, ибо мудрость у каждого больше зависит от знания, и это потому, что первые знают причину, а вторые нет.

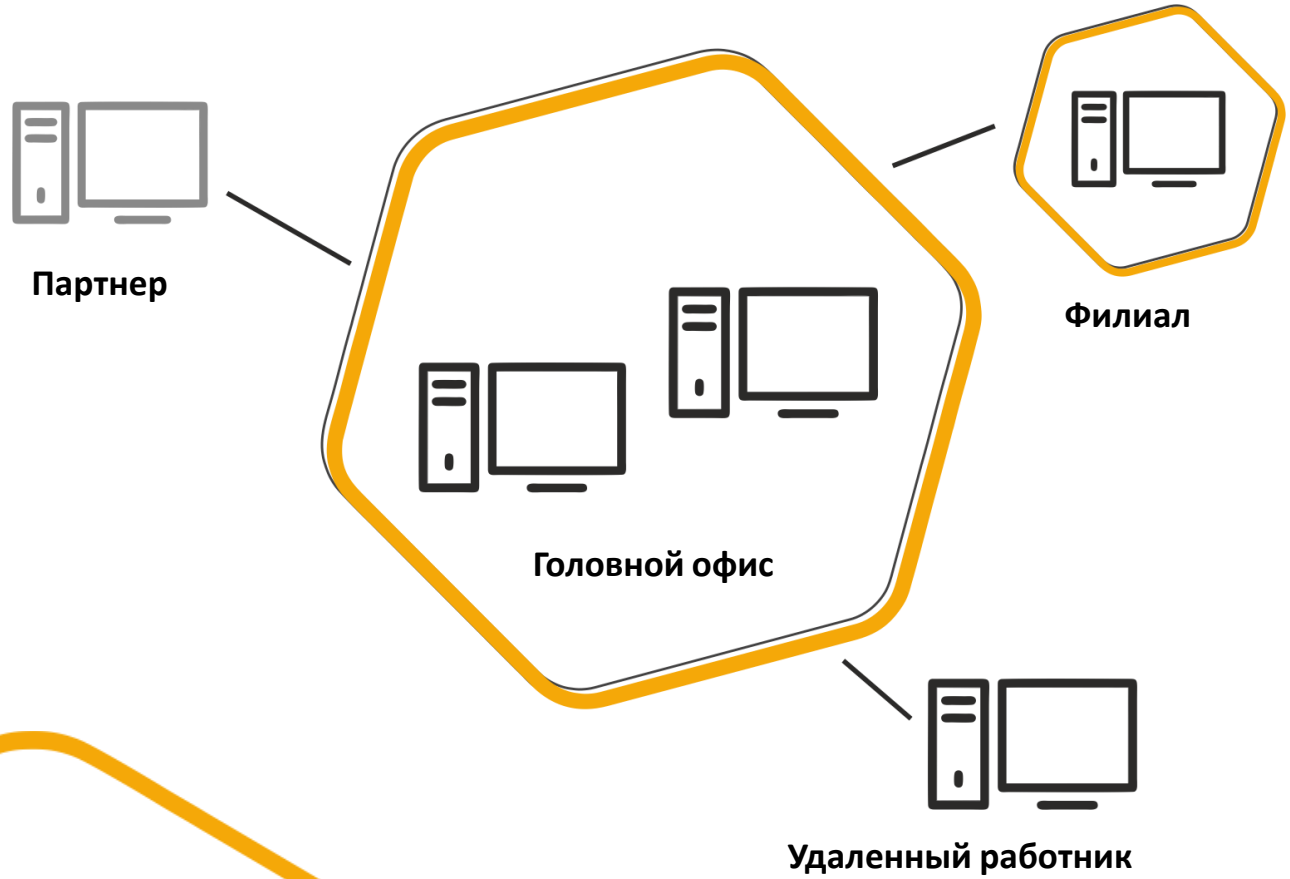
Аристотель

Настоящее



Безопасность не продукт – а процесс
Б. Шнайер

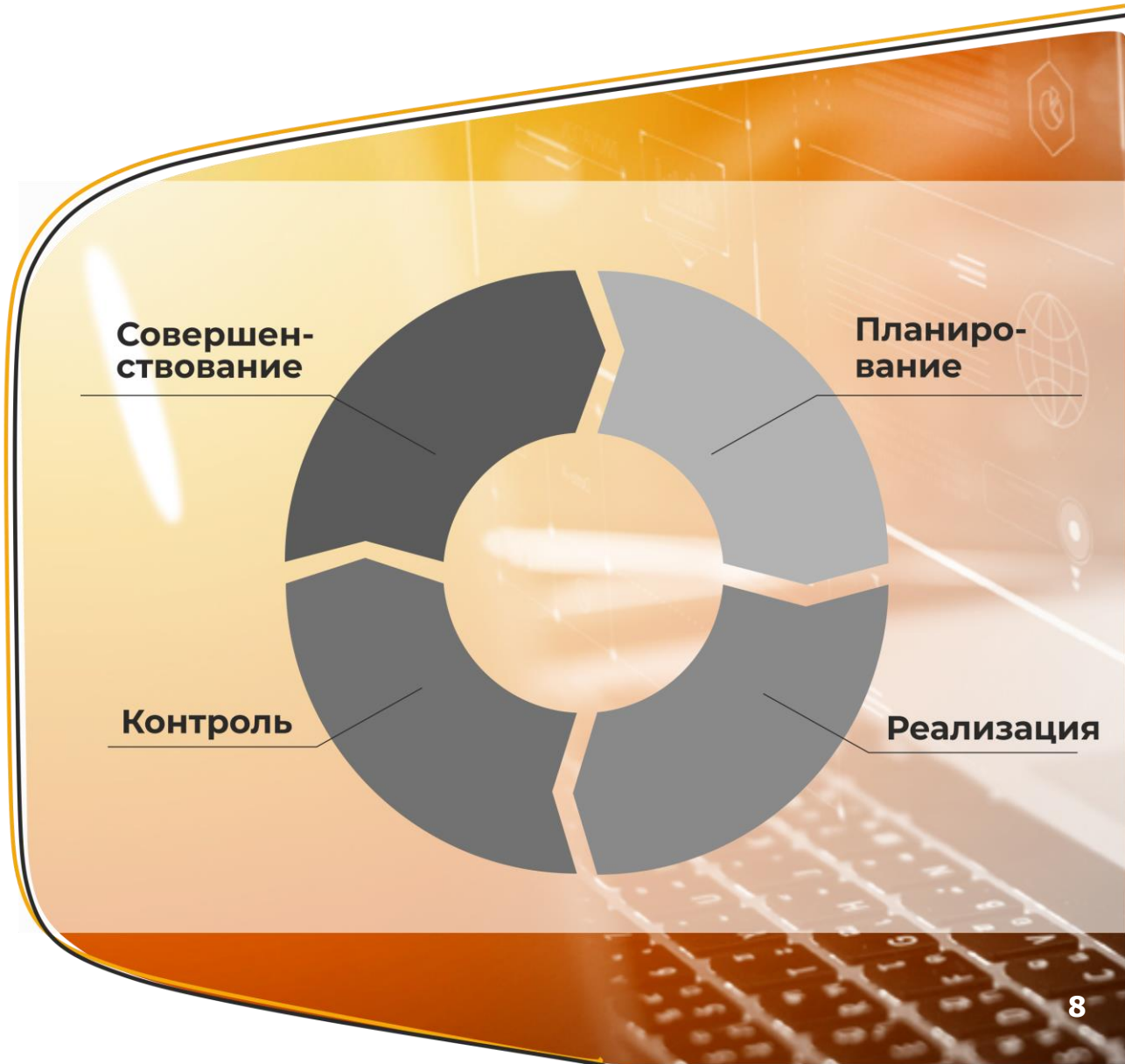
Модель «Аэропорт»



- Информационные системы выросли, как и зависимость бизнеса от них
- Периметра нет – сеть без границ
- Все потоки контролировать невозможно
- Не хватает кадров, времени, материальных ресурсов… всего

Парадигма ИБ эпохи «Аэропортов»

- Управление рисками – основа системы обеспечения ИБ
- В основе СОИБ процессы и люди, а не технические средства
- ИБ для бизнеса, а не наоборот
- Система должна уметь быстро меняться (в том числе, СОИБ)
- Готовых рецептов нет, но есть ряд обязательных требований
- Уход от невзламываемой системы к быстрому обнаружению атаки (ability to detect)



Требуемые знания и навыки специалиста по ИБ

Прикладные знания

- Системы управления сетевым доступом
- Системы анализа событий ИБ
- Системы управления оконечными устройствами
- Сетевые технологии
- Законодательство в области ИБ
- Системы контроля информационных потоков
- Системы управления оконечными устройствами

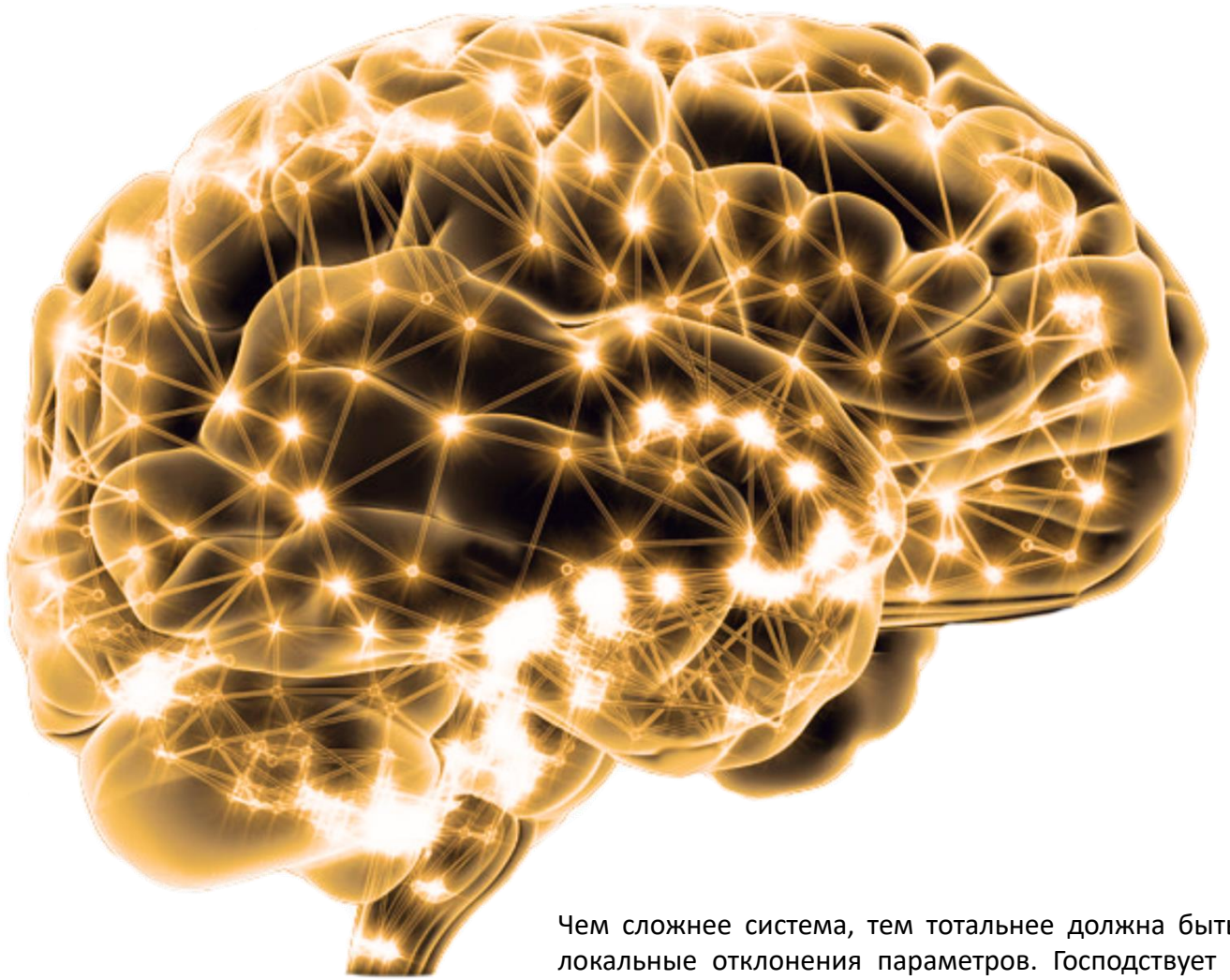
Фундаментальные знания

- Формальные модели управления доступом
- Политика ИБ
- Порядок создания АС в ЗИ
- Цикл Деминга
- Риск-ориентированный подход
- Монитор безопасности
- Принципы пакетной передачи данных
- Свойства безопасности информации
- Комплексная СОИБ

...в современном промышленном обществе существует отчетливая граница между теми, кто обслуживает устройства (рабочие, техники) или пользуется ими (человек в лифте, у телевизора, за рулем автомашины), и теми, кто знает их конструкцию. Ни один из ныне живущих не знает устройства всех орудий, которыми располагает цивилизация.

С. Лем

Будущее



Чем сложнее система, тем тотальнее должна быть ее регулировка, тем менее допустимы локальные отклонения параметров. Господствует ли наш мозг как регулятор над нашим телом? Безусловно. Господствуем ли мы сами, каждый из нас, над своим телом? Только в очень узком диапазоне параметров

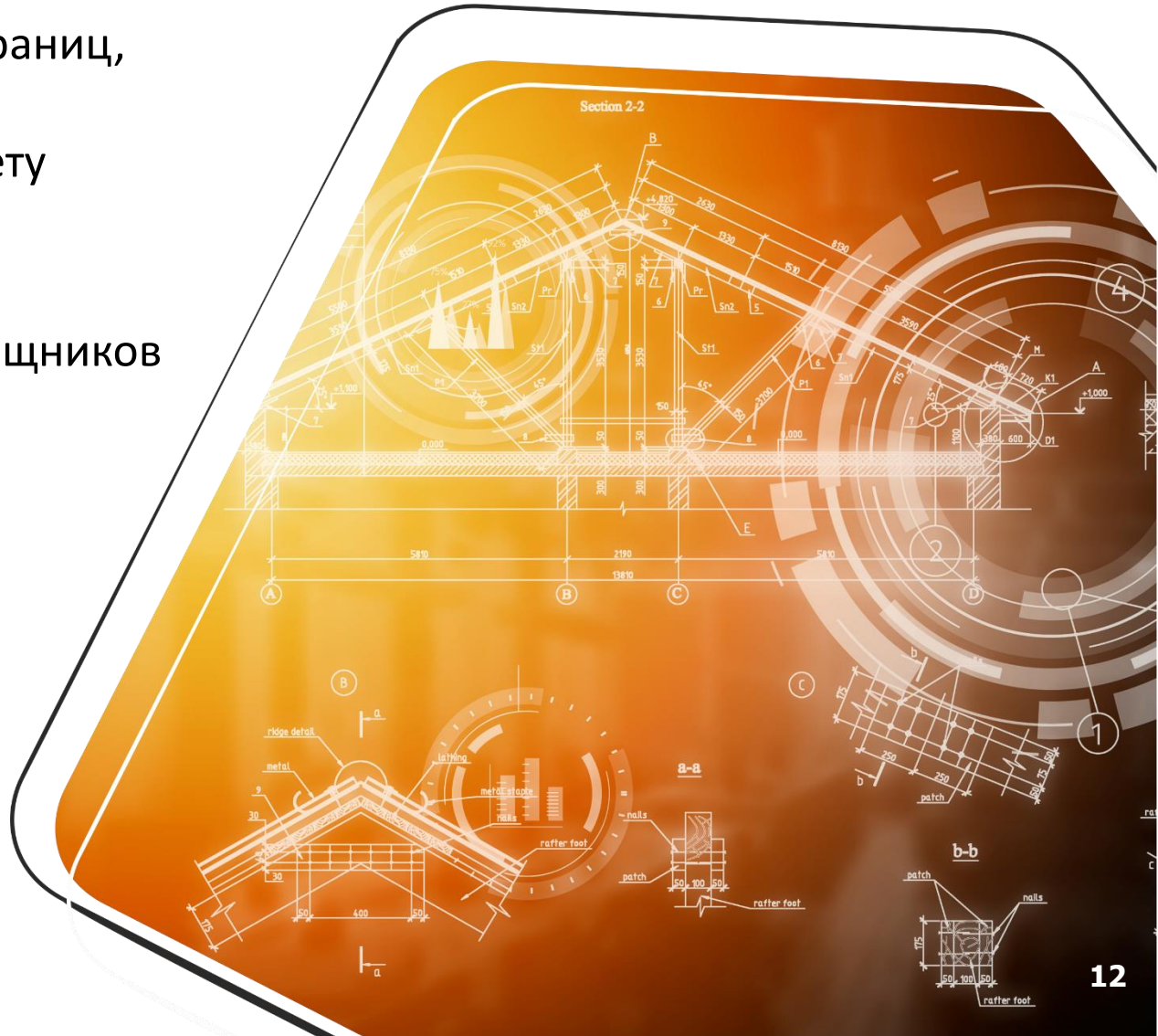
С. Лем

Модель «Черный ящик»

- Уход от прямого управления инфраструктурой информационных систем (SDN, облака)
- Реализация полностью автономных систем
- Повсеместное внедрение технологий искусственного интеллекта
- Когнитивные архитектуры и «сильный» ИИ

Парадигма ИБ эпохи «Черного ящика»

- Информационная система не имеет не только границ, но и локации
- От возможности обнаружения к кибериммунитету (Cyberimmunity)
- Роль человека – наблюдатель и координатор
- Создание СОИБ = обучение искусственных помощников
- Грань между инженером, программистом или аналитиком сотрется
- Новая область – защита искусственного интеллекта от угроз ИБ



Требуемые знания и навыки специалиста по ИБ

Прикладные знания

- Законодательство в области ИБ и ИИ
- Алгоритмы и методы машинного обучения
- Создание целеориентированных систем

Фундаментальные знания

- Политика ИБ
- Автономные вычисления
- Искусственный интеллект
- Комплексная СОИБ
- Риск-ориентированный подход
- Теория управления

Требуемые знания и навыки специалиста по ИБ

Прикладные знания

Законодательство в области ИБ и ИИ

Алгоритмы и методы машинного обучения

Создание целеориентированных

Умение быстро и много учиться

Комплексная СОИБ

Риск-ориентированный подход

Теория управления

Нет стремления более естественного, чем стремление к знанию…
М. Монтень

УЦСБ

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Николай Домуховский

Заместитель генерального директора по научно-технической работе

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU