AKTIV.
CONSULTING

Бизнес-завтрак

Роль ИБ в компании:
издержки или дополнительные выгоды?

Дмитрий Ли
Независимый эксперт

Как ИБ-подразделение видят коллеги

- Люди, которые занимаются непонятно чем и генерируют бесполезную работу для других
- Сапоги и фуражка: есть устав и жизнь надо по нему
- Надзиратели и каратели
- Жители страны розовых пони и единорогов, которые только и могут, что фантазировать и рассказывать страшилки
- Паразиты и проедатели бюджета

Чтобы изменилось восприятие ИБ, нужны качественные изменения

Как сделать качественный переход?

Ценность результатов работы ИБ-подразделения должна быть очевидна и ощутима не только для ИБ.

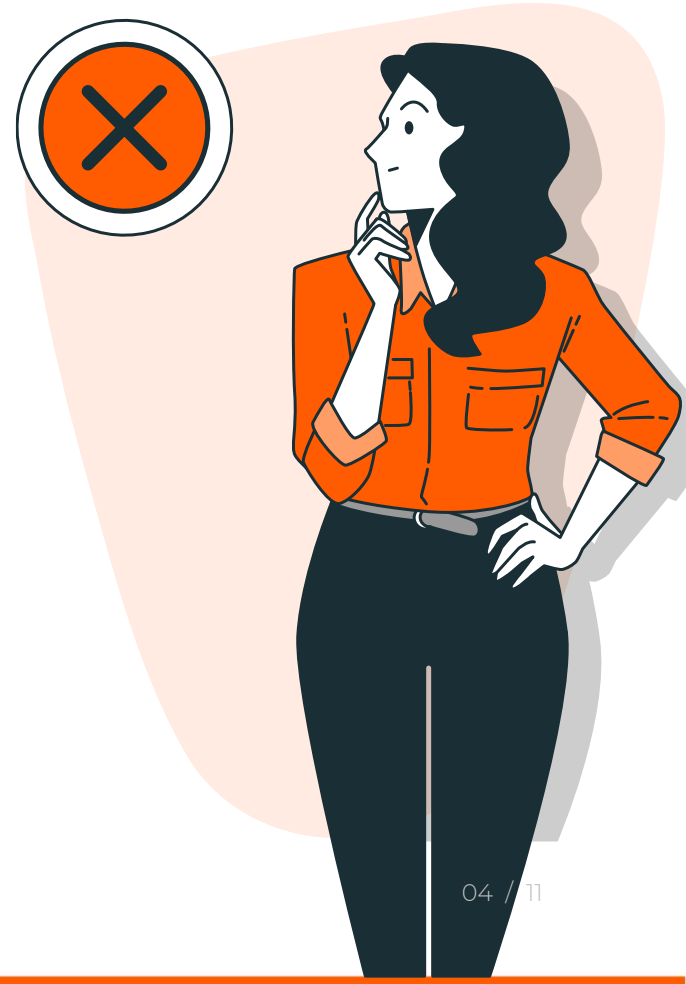
Задачи для качественного перехода:

- Инвентаризация активов
- Управление правами доступа
- Управление *[неструктурированными]* данными, оптимизация и хранение

Инвентаризация – базис для обеспечения ИБ

Нельзя построить систему защиты чего-либо, **не понимая, что требуется защитить:**

- некорректная оценка угроз безопасности информации
- недостаток конфигурационных контролей для ИТ-активов
- неэффективное управление обновлениями
- неэффективное управление уязвимостями
- ...



СЗИ – источник сведений об ИТ-активах

Что это дает **для ИБ-подразделений и организации в целом:**

- доступ к актуальной информации в любой момент
- повышение достоверности сведений
- возможность построения процессов управления обновлениями
- снижение трудозатрат как для ИБ, так и для ИТ-подразделений
- снижение издержек на покупку систем с похожим функционалом
- повышение прогнозируемости управления ИТ-инфраструктурой

*возможность для выстраивания конструктивного диалога со смежными подразделениями

Управления правами доступа.
Действительно контролируем или это самообман?

Управление доступом комплексная задача

Проблемы ИБ	Проблемы ИТ	Проблемы пользователей и бизнеса
Отсутствия доступа ко всем ресурсам	Массовые запросы, связанные с правами доступа	Нет понимания, как запросить и получить доступ
Мертвые души	Трудоемкая рутина	Непрозрачен процесс предоставления прав доступа
Непрозрачна процедура присвоения прав доступа и их пересмотра	Не понятно, чего хочет пользователь	Отсутствие информации у бизнес-владельцев ресурсов о правах доступа
Отсутствие информации об изменениях прав доступа	Отсутствие единого окна	Доступ к чувствительной информации
Процедуры прав доступом фактически не работают	Конфликты с ИБ	SoD-конфликты

Внедряем IDM силами ИБ

Снижаем энтропию путем автоматизации процессов управления доступами и жизненным циклом учетных записей.

Профиты от внедрения IDM:

- ИБ-подразделение получает единый инструмент, позволяющий осуществлять контроль существующих прав доступа и историю их изменений;
- Снижается нагрузка на ИТ-подразделение;
- Снижаем риски появления инцидентов, связанных с человеческим фактором.

Для пользователей и бизнеса:

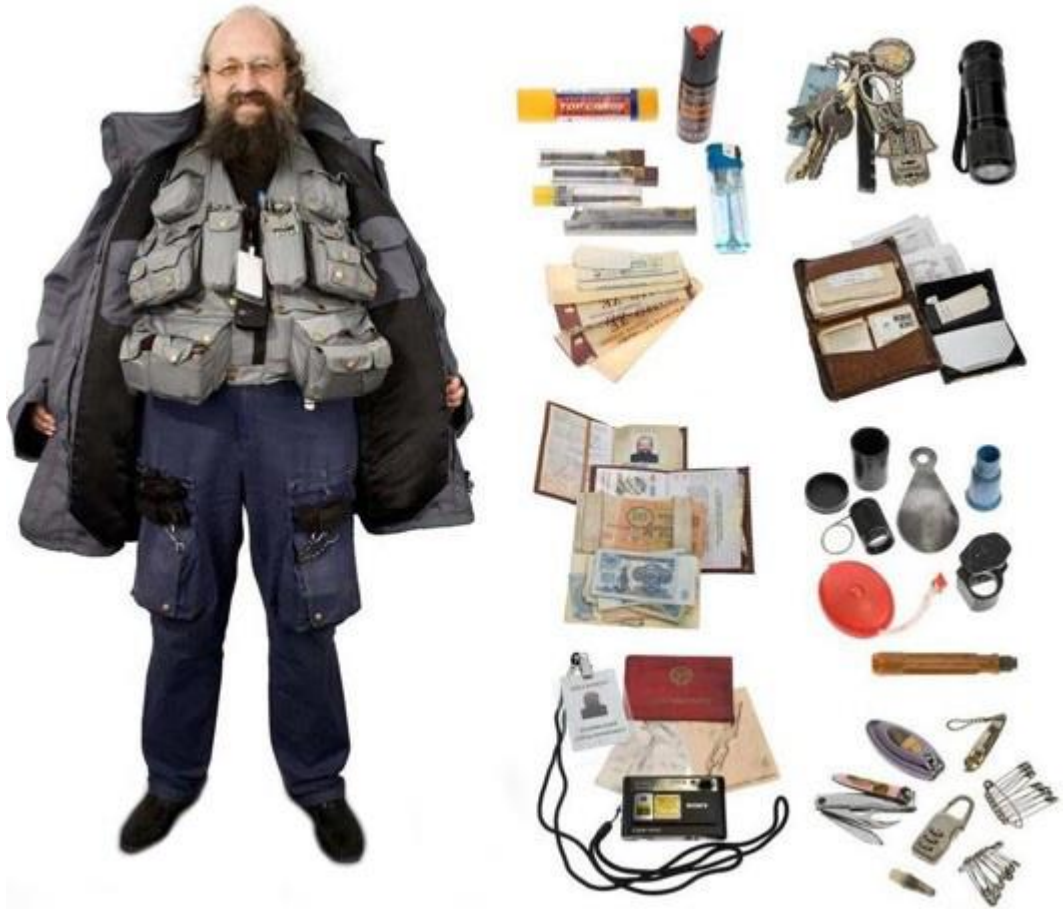
- Повышение эффективности работы сотрудников;
- Избежание SoD-конфликтов;
- Возможность для выстраивания конструктивного диалога со смежными подразделениями.

ИБ не просит, ИБ приносит пользу!

Управление данными.
Многие знания - многие печали

Распространенная ситуация:

- критичные данные хранятся на общем ресурсе (например, ПДн)
- данные многократно дублируются
- невозможно проконтролировать распространение данных
- наряду с «полезными» данными хранятся личные данные пользователей



Если не можешь победить хаос, возглавь его...

DCAP (Data-Centric Audit and Protection) — это контентное разграничение доступа: не по объектам файловой системы, а по содержимому.

Какие профиты мы получаем:

- Снижаем количество инцидентов, связанных с утечками данных;
- Выполняем требования регуляторов (ФЗ-152, требования ФСТЭК и так далее) и избегаем штрафов за их несоблюдение;
- Экономим средства компании за счет:
  - автоматизации работы ИБ-подразделений;
  - оптимизации файловых хранилищ.

*Получаем возможность для выстраивания конструктивного диалога со смежными подразделениями.

AKTIV.
CONSULTING

Дмитрий Ли

Независимый эксперт