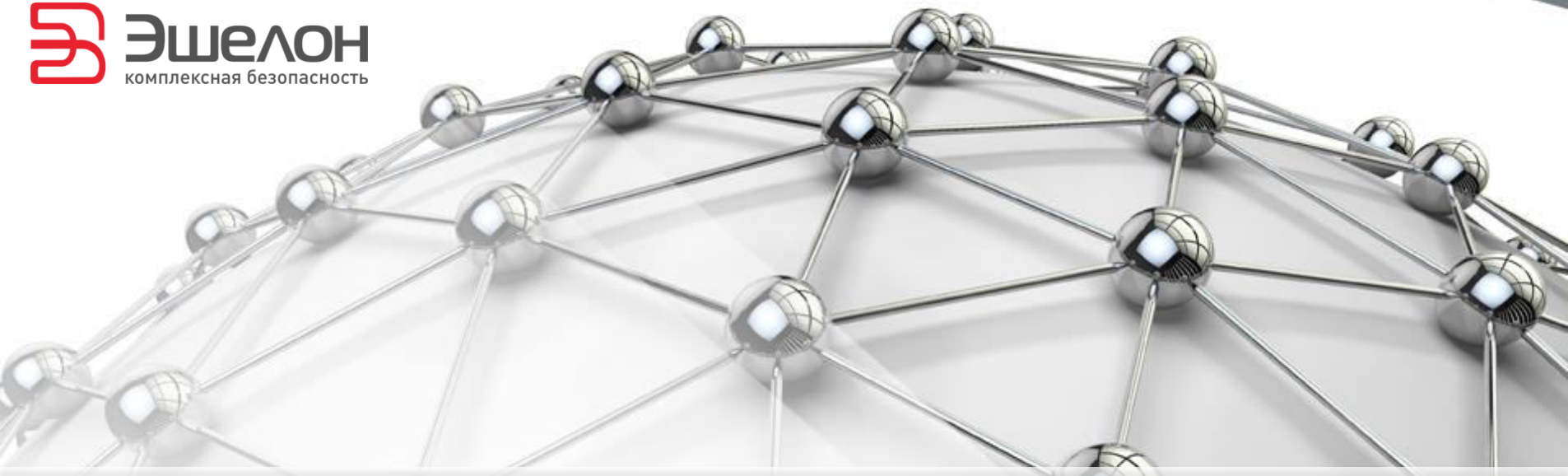
Эшелон
комплексная безопасность



Аудит информационной безопасности: все, что вы хотели узнать, но боялись спросить

Александр Дорофеев
CISSP, CISM, CISA
Директор по развитию

Аудит - систематический, независимый и документированный процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения согласованных критериев аудита

Критерии аудита ИБ

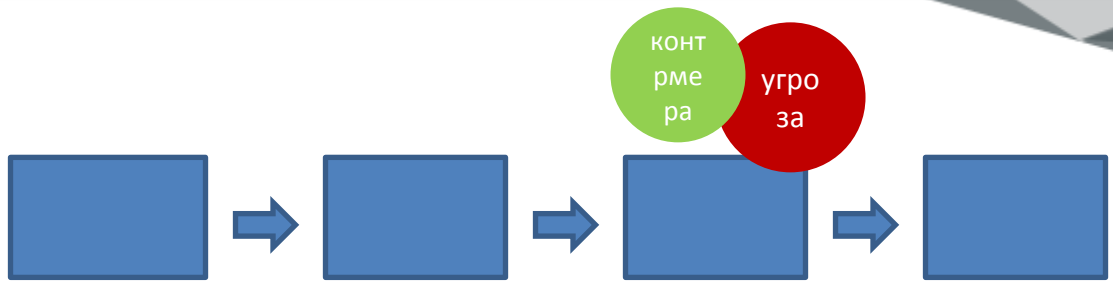
Процессы	• требования корпоративных политик, международных стандартов, законодательства: ISO 27001, COBIT
Технологии	• уровень защищенности информационных систем от внутренних и внешних злоумышленников
Люди	• способность сотрудников противостоять действиям злоумышленников, пытающихся с помощью обмана получить конфиденциальную информацию

Процессы

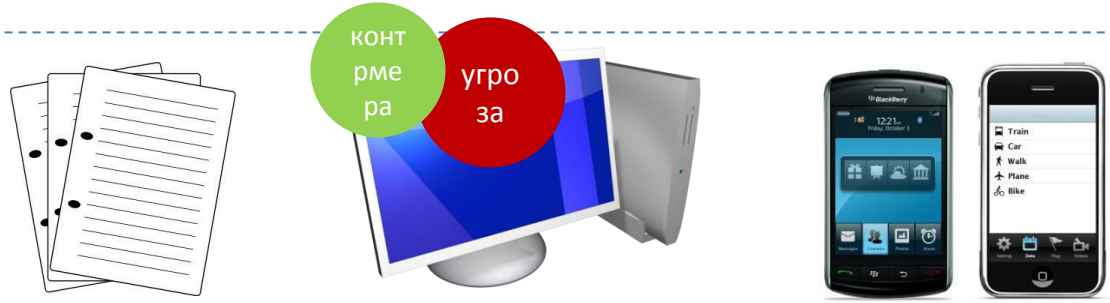
Эшелон
комплексная безопасность

Границы аудита – могут определяться подразделениями, процессами, системами

процессы



технологии



люди

Эшелон
комплексная безопасность

Оценка процессов и контролей в процессах

ISO 19011: Ключевые виды деятельности

6.2 Подготовка к аудиту

6.2.1 Общие сведения
6.2.2 Установление первоначального контакта с проверяемым
6.2.3 Определение возможности проведения аудита

6.3 Планирование аудита

6.3.1 Проведение анализа документации при подготовке к аудиту
6.3.2 Подготовка плана аудита
6.3.3 Распределение работы в команде аудита
6.3.4 Подготовка рабочих документов

6.4 Проведение аудита

6.4.1 Общие сведения
6.4.2 Вступительное совещание
6.4.3 Проверка документации в ходе аудита
6.4.4 Коммуникации в ходе аудита
6.4.5 Роли и ответственности сопровождающих и наблюдателей
6.4.6 Сбор и проверка информации
6.4.7 Формулировка выявлений аудита
6.4.8 Подготовка заключения аудита
6.4.9 Заключительное совещание

6.5 Подготовка и распространение отчета по аудиту

6.5.1 Подготовка отчета по аудиту
6.5.2 Распространение отчета по аудиту

6.6 Завершение аудита

6.7 Отслеживание результатов аудита

Эшелон
комплексная безопасность

Методы аудита

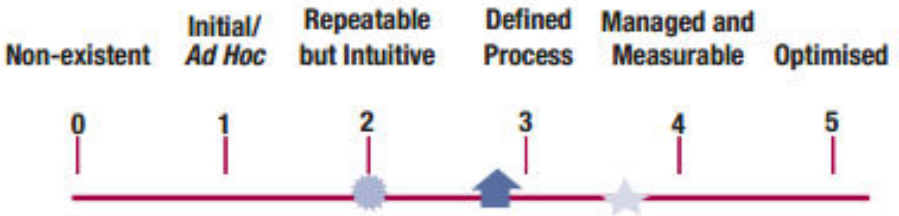
1) Наблюдение
2) Интервью
3) Разовый проход по процессу (walkthrough)
4) Выборочное тестирование
5) Полное тестирование

Бинарная оценка: «неэффективная» или «эффективная» контрмера

Эшелон
комплексная безопасность

Оценка зрелости процессов

Figure 12—Graphic Representation of Maturity Models



LEGEND FOR SYMBOLS USED

- Enterprise current status
- Industry average
- Enterprise target

LEGEND FOR RANKINGS USED

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

источник: Cobit

Эшелон
комплексная безопасность

Аудит СМИБ: несоответствие

Невыполнение установленного требования в…

- ✓ Политике безопасности
- ✓ Стандарте ISO 27001
- ✓ Процедурах и процессах СМИБ
- ✓ Целевых показателях результативности процессов или средств управления
- ✓ Законодательных и нормативных актах

Оценка масштабов несоответствия

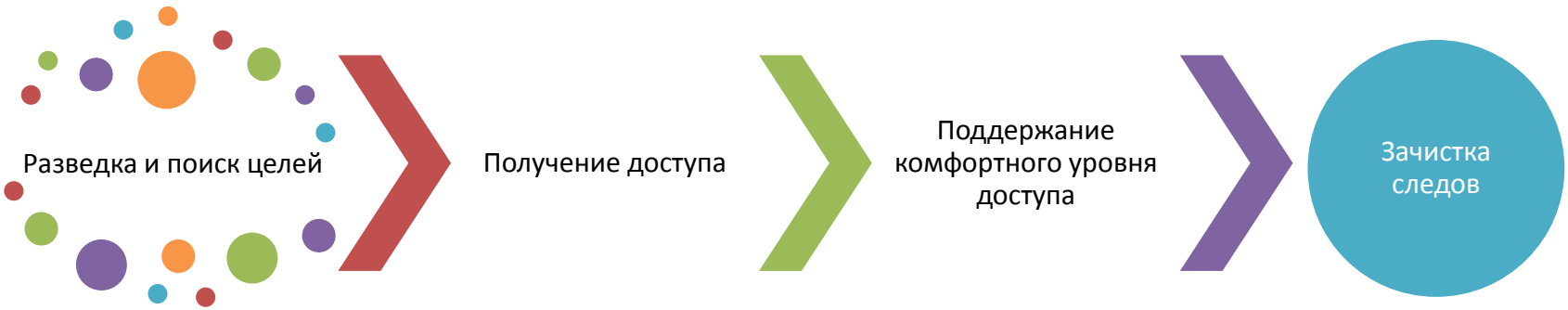
Незначительное

Значительное

Технологии

Эшелон
комплексная безопасность

Что делает настоящий хакер?



Эшелон
комплексная безопасность

Что можно взять для аудита?

- ✓ Модель злоумышленника
- ✓ Цели
- ✓ Инструменты
- ✓ Методики

Модель злоумышленника

- ✓ **Возможности злоумышленника:**
  - Применение известных хакерских утилит
  - Применение хакерских методик
  - Связи с «черным рынком»
  - Возможность самостоятельного поиска zero-day
  - Возможность разработки собственных средств (например, эксплойтов).

Цели

Административный доступ к системам

Доступ к определенной информации: финансы, электронная почта, ноу хау и т.п.

Эшелон
комплексная безопасность

Инструментарий «этичного» хакера

или

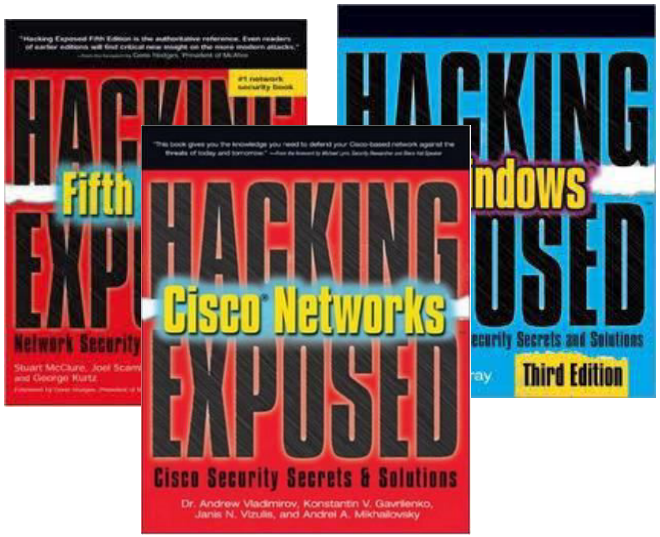
Linux
Windows
+ Хакерские утилиты

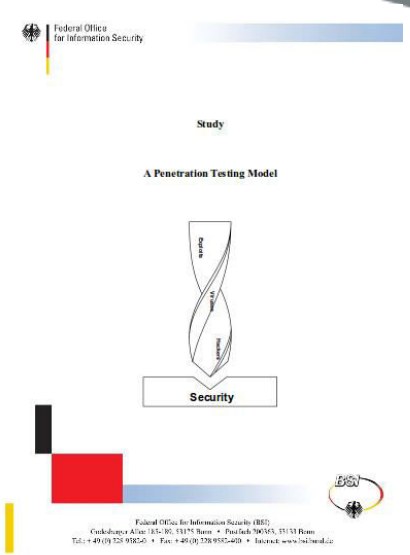
Загрузочный носитель с Linux
и предустановленные утилиты
Примеры: Kali Linux, Сканер-ВС

«Хакерские» утилиты

- ✓ Встроенные сетевые утилиты для работы с DNS, whois, ICMP и др.
- ✓ Сканеры портов
- ✓ Сканеры уязвимостей
- ✓ Утилиты для работы с различными сетевыми протоколами Netcat
- ✓ Утилиты для идентификации конкретных уязвимостей
- ✓ Наборы эксплойтов
- ✓ и т.д. и т.п.

Методологии





Эшелон
комплексная безопасность

Подходы к оценке защищенности

Классический тест на проникновение

Сканирование на наличие уязвимостей

Анализ конфигурации системы

Комплексный подход

Эшелон
комплексная безопасность

Классический тест на проникновение

- Имитация действий реального злоумышленника – поиск первой уязвимости, позволяющей получить доступ к системе
- Больше искусство, чем аудит. Качество сильно зависит от уровня специалиста
- Обычный результат: несколько опасных уязвимостей
- Высокий риск нарушения доступности систем

Эшелон
комплексная безопасность

Сканирование

- Использование исключительно сканеров для поиска уязвимостей
- Качество сильно зависит от используемого сканера.
- Результат: множество уязвимостей различного уровня опасности
- Средний риск нарушения работоспособности систем

Эшелон
комплексная безопасность

Анализ конфигурации системы

- Проверка настроек систем в соответствии с рекомендуемыми вендорами или сообществами профессионалов по ИБ (NIST, Center of Internet Security).
- Результат: множество уязвимостей различного уровня опасности
- Низкий риск нарушения работоспособности систем

Чеклисты для анализа конфигурации

http://benchmarks.cisecurity.org/downloads/

http://web.nvd.nist.gov/view/ncp/information

Комплексное тестирование

Эшелон
комплексная безопасность

Управление проектом

- ✓ Согласование перечней IP-адресов: критичные/некритичные
- ✓ Согласование подхода
- ✓ Получение подтверждений/разрешений от провайдеров
- ✓ Согласование в процессе эксплуатации
- ✓ Отчетные материалы

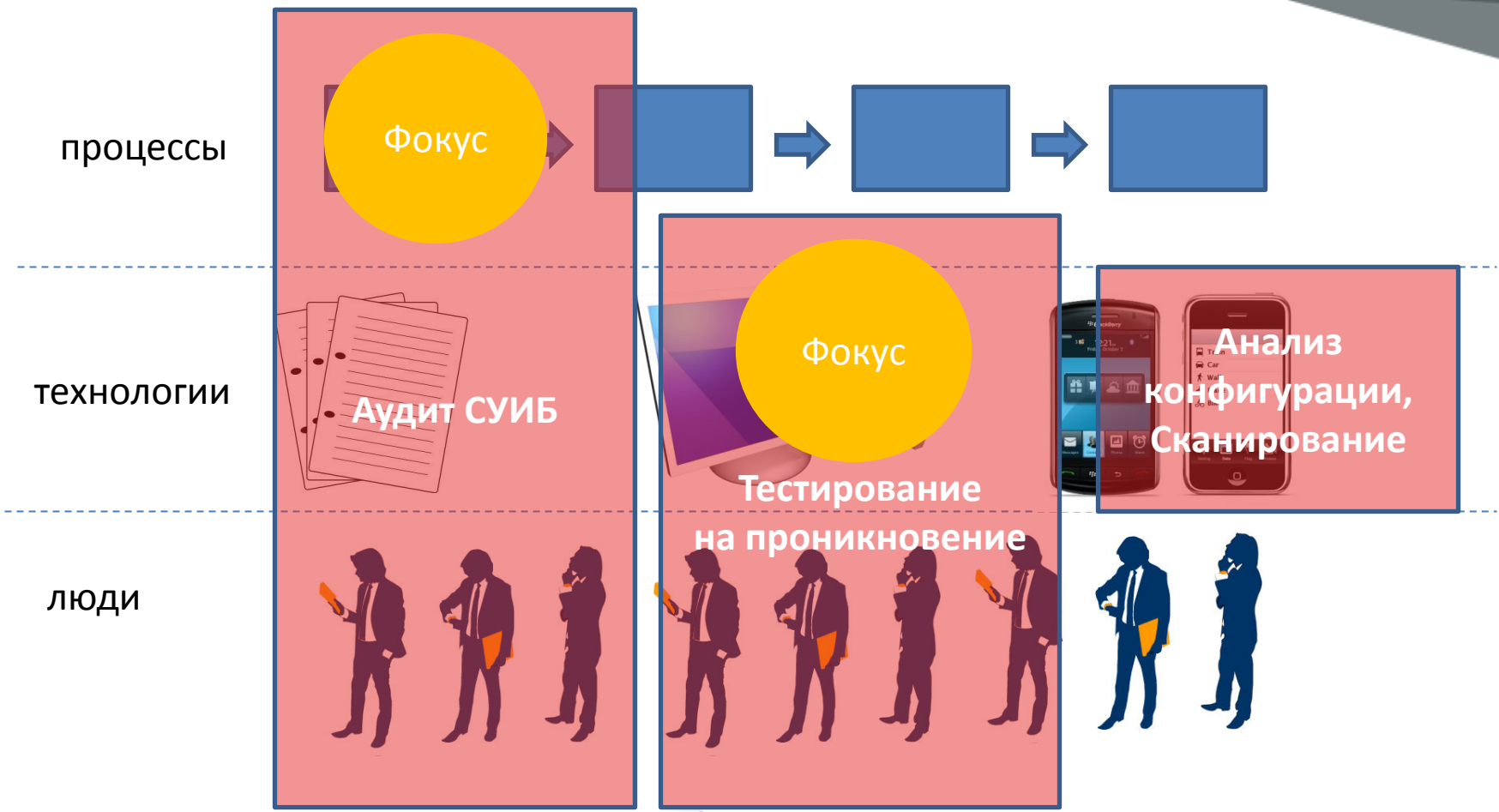
Люди

Эшелон
комплексная безопасность

Примеры

- Провокационные письма с просьбой сообщить пароль
- Фишинг-атаки
- и др.

Границы аудита и фокус



Эшелон
комплексная безопасность

Формат отчета

Finding – Risk – (Recommendation)

Эшелон
комплексная безопасность

Контактная информация

107023, Москва, ул. Электрозаводская, д. 24

+7(495) 223-23-92
+7(495) 645-38-11

http://www.uc-echelon.ru

mail@uc-echelon.ru