Лекция 11.
Аудит безопасности и резервное базы данных

- Рассмотреть понятие аудита информационной безопасности
- Выделить основные этапы проведения аудита безопасности
- Изучить способы проведения аудита безопасности

Услуги по проведению аудита информационной безопасности

- Перед внедрением комплексной системы безопасности для подготовки текущего уровня на её разработку и создание
- После внедрения комплексной системы безопасности для оценки уровня её эффективности
- Для приведения системы информационной безопасности в соответствие установленным требованиям (международные стандарты или требования законодательства)
- Для систематизации и упорядочивания существующих мер защиты информации
- Для обоснования инвестиций в направление информационной безопасности

Конечные потребители результатов аудита

Внутренние пользователи:

- Руководство компании
- Служба информационной безопасности
- Служба автоматизации предприятия
- Служба внутреннего контроля/аудита

Внешние пользователи:

- Акционеры компании
- Регулирующие органы
- Страховые компании
- Клиенты компании

Варианты проведения аудита

- Инструментальный анализ защищённости автоматизированной системы
- Аудит безопасности Интернет-систем (penetration testing)
- Аудит безопасности, направленный на оценку соответствия требованиям стандарта ISO 27001 (ISO17799)
- Оценка соответствия стандарту Банка России
- Аудит наличия конфиденциальной информации в сети Интернет
- Оценка и анализ рисков информационной безопасности
- Комплексный аудит информационной безопасности

Основные этапы работ

- Заключение соглашения о неразглашении (NDA)
- Разработка регламента, устанавливающего порядок и рамки проведения работ
- Сбор исходной информации об автоматизированной системе компании
- Анализ собранной информации с целью выявления технологических, эксплуатационных уязвимостей, а также недостатков организационно-правового обеспечения
- Подготовка отчётных материалов
- Презентация и защита результатов проекта

Варианты проведения аудита

- Инструментальный анализ защищённости автоматизированной системы
- Аудит безопасности Интернет-систем (penetration testing)
- Аудит безопасности, направленный на оценку соответствия требованиям стандарта ISO 27001 (ISO17799)
- Оценка соответствия стандарту Банка России
- Аудит наличия конфиденциальной информации в сети Интернет
- Оценка и анализ рисков информационной безопасности
- Комплексный аудит информационной безопасности

Инструментальный анализ защищенности

Для чего предназначен:

- Инвентаризация ресурсов сети (устройства, ОС, службы, ПО)
- Идентификация и анализ технологических уязвимостей
- Подготовка отчетов, описание проблем и методов устранения

Типы используемых для анализа средств:

- Сетевые сканеры безопасности
- Хостовые сканеры безопасности (проверка ОС и приложений)
- Утилиты удаленного администрирования
- Утилиты для верификации найденных уязвимостей
- Утилиты для инвентаризации ресурсов

Инструментальный анализ защищенности

- Анализ средств защиты информации
  - Анализ VPN-шлюзов
  - Анализ антивирусных средств защиты
  - Анализ систем обнаружения атак IDS/IPS
  - Анализ межсетевых экранов
  - Анализ систем защиты от утечки конфиденциальной информации
- Анализ безопасности сетевой инфраструктуры
  - Анализ безопасности коммутаторов
  - Анализ безопасности маршрутизаторов
  - Анализ безопасности SAN-сетей
  - Анализ безопасности сетей WLAN

Инструментальный анализ защищенности

- **Анализ безопасности общесистемного программного обеспечения**
  - Анализ ОС Windows
  - Анализ ОС UNIX
  - Анализ ОС Novell Netware

- **Анализ безопасности прикладного программного обеспечения**
  - Анализ безопасности баз данных
  - Анализ безопасности почтовых серверов
  - Анализ безопасности Web-серверов
  - Анализ безопасности Web-приложений

Особенности использования инструментальных средств для сбора информации

- Заранее оговариваются рамки проведения инструментального аудита
- Результаты анализируются и интерпретируются экспертами
- Производится фильтрация полученных данных
- Проверку критически важных систем желательно проводить во внерабочие часы, в присутствии администратора с обязательным резервным копированием информации

Тест на проникновение (Penetration testing)

Тест на проникновение позволяет получить независимую оценку безопасности компании глазами потенциального злоумышленника

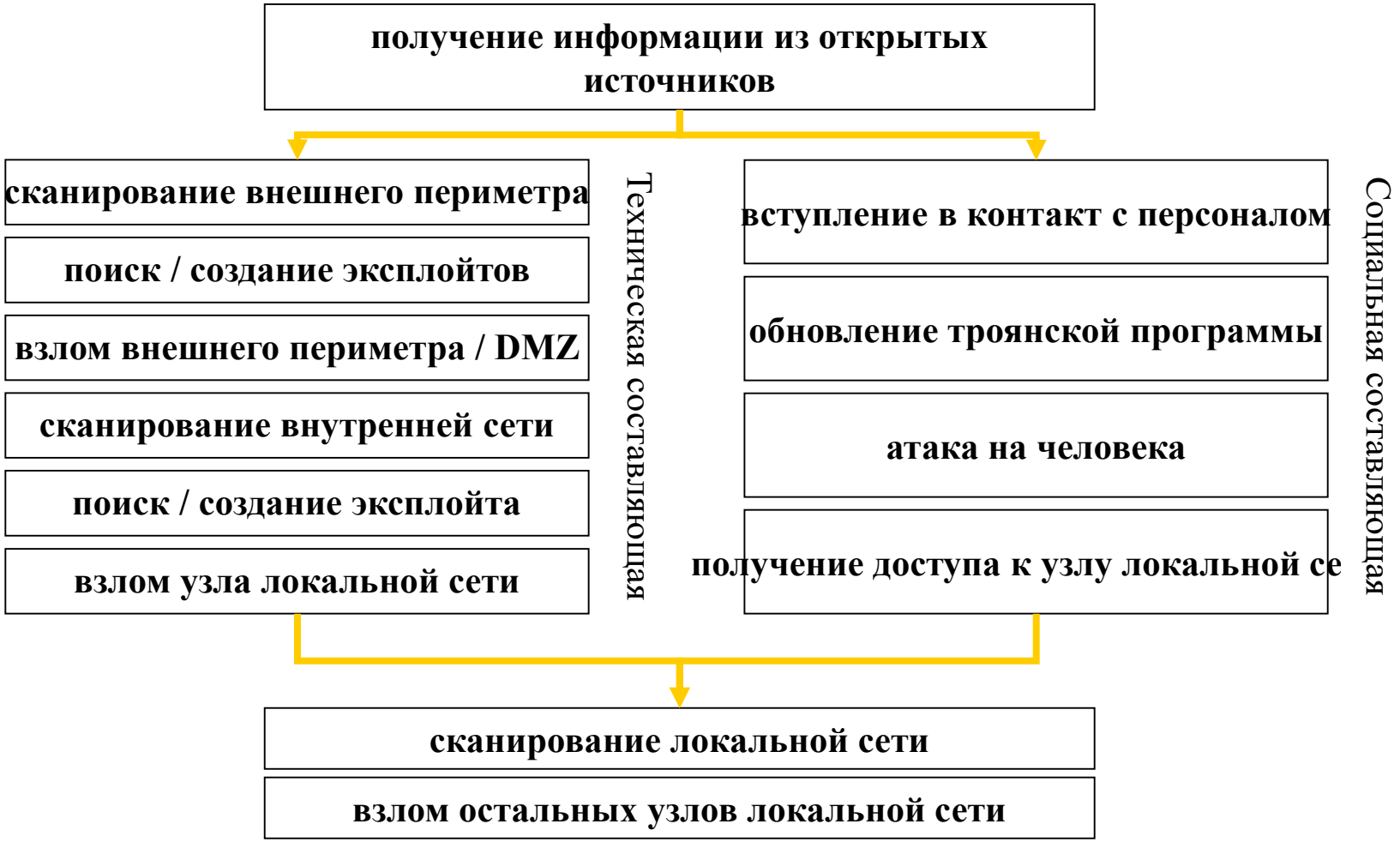
Исходные данные

- IP-адреса внешних серверов
- Анализ проводится с внешнего периметра

Собираемая информация

- Топология сети
- Используемые ОС и версии ПО
- Запущенные сервисы
- Открытые порты, конфигурация и т.д.

Обобщенный план удаленного аудита



Оценка соответствия стандарт Банка страны

- Определение текущего уровня информационной безопасности организации банковской системы страны
- Определение тенденции в обеспечении информационной безопасности организации банковской системы страны
- Определение уровня осознания значения информационной безопасности для деятельности организации банковской системы страны

Определение текущего уровня информационной безопасности

- Назначение и распределение ролей, обеспечение доверия к персоналу
- Автоматизированные банковские системы на стадиях жизненного цикла
- Управление доступом и регистрация
- Средства антивирусной защиты
- Использование ресурсов сети Интернет
- Средства криптографической защиты

Определение тенденции в обеспечении информационной безопасности

- Определение области действия систему управления информационной безопасностью
- Оценка и обработка рисков информационной безопасности
- Реализация программы по обучению информационной безопасности
- Обнаружение и реагирование на инциденты в области информационной безопасности
- Мониторинг и контроль защитных мер
- Информирование об изменениях системы управления информационной безопасности

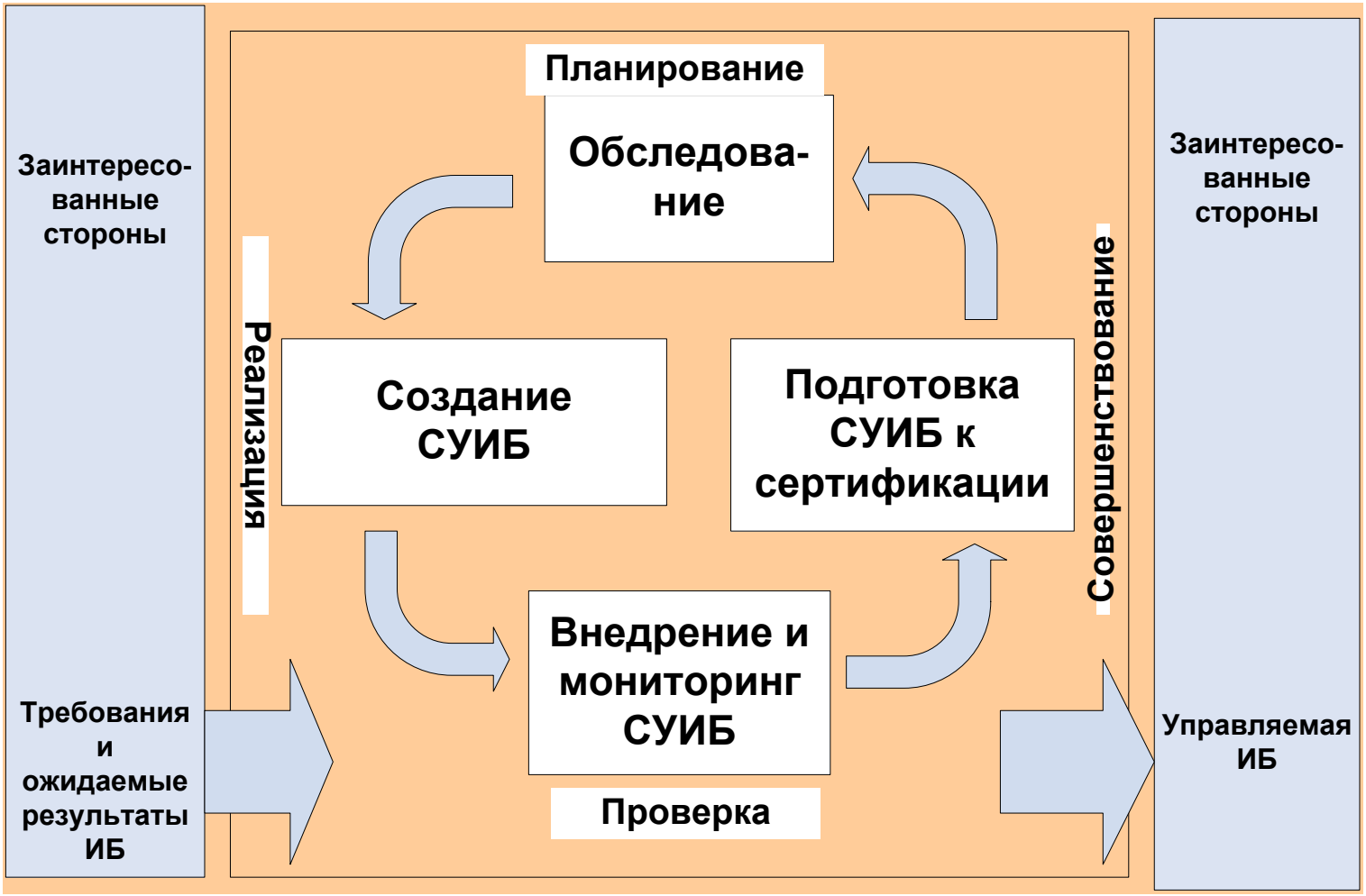
Определение уровня осознания значения информационной безопасности

- Определение своевременности обнаружения, прогноза развития проблем информационной безопасности
- Определение наблюдаемости и оцениваемости обеспечения информационной безопасности
- Определение доступности услуг и сервисов
- Персонификация и адекватное разделение ролей и ответственности
- Оценка определённости целей, адекватности выбора защитных мер, их эффективности и контролируемости

Аудит СУИБ по стандарту ISO 27001

1. Политика безопасности
2. Организационные меры безопасности
3. Учет и категорирование информационных ресурсов
4. Кадровые аспекты ИБ
5. Физическая защита информационных ресурсов
6. Управление технологическим процессом
7. Управление доступом
8. Закупка, разработка и сопровождение компонент ИС
9. Управление инцидентами в области информационной безопасности
10. Обеспечение непрерывности работы и восстановления
11. Соответствие нормативным и руководящим документам

Оценка соответствия ISO 27001



Аудит наличия конфиденциальной информации

Аудит наличия конфиденциальной информации представляет собой независимый и документированный процесс поиска и анализа конфиденциальных сведений в сети Интернет при помощи средств конкурентной разведки

- Поиск информации осуществляется: на форумах, в блогах, в электронных СМИ, в гостевых книгах, на досках объявлений, в дневниках, конференциях и т.д.
- По результатам проведённого поиска проводится выдача «оценочной» информации в виде отчёта. Отчёт содержит следующую информацию:
    1. область поиска (где осуществлялся поиск);
    2. найденная конфиденциальная информация;
    3. где найдена конфиденциальная информация;
    4. рекомендации по устранению (удалению) найденной конфиденциальной информации в Интернете

Оценка и анализ рисков безопасности

- Идентификация информационных активов
- Формирование каталога возможных угроз безопасности
- Оценка уровня вероятности реализации угроз безопасности
- Оценка уровня ущерба, который может быть нанесен в случае реализации угрозы
- Определение интегрального значения риска безопасности
- Анализ рисков безопасности

Комплексный аудит безопасности

- Учитывает организационные и технологические аспекты защищённости автоматизированной системы компании
- Предполагает проведение оценки рисков информационной безопасности
- Учитывает требования российского законодательства и рекомендации международных стандартов
- При необходимости может включать в себя инструментальное обследование организации

Преимущества аудита безопасности

- Лучшее понимание руководством и сотрудниками целей, задач, проблем организации в области ИБ
- Осознание ценности информационных ресурсов
- Надлежащее документирование процедур и моделей ИС с позиции ИБ
- Принятие ответственности за остаточные риски