Организация корпоративной защиты от вредоносных программ

Алексей Неверов

Пермский государственный университет,

кафедра Процессов управления и информационной безопасности

Вредоносные программы

- Вирусы («классические» вирусы)
  - Файловые
  - Загрузочные
- Программы-черви
- Программы-трояны («троянские кони»)
- Вредоносные программы смешанного типа

Вирусы

- Для распространения используют код, прикрепленный к объекту-носителю (программе, документу, загрузочной области и т.д.)
- Выполняют вредоносные действия
- Самостоятельно распространяются за счет заражения новых носителей, возможно, на других компьютерах

Программы-трояны

- Безобидные с виду программы, выполняющие полезные действия, но содержащие вредоносный код
- Основной способ распространения – рассылка по сети (сбрасывание)
- Технологии троянов часто используются в «полезных» программах (удаленного управления, мониторинга), но это ведет к снижению уровня безопасности системы

Программы-черви

- Программы, способные к самостоятельному копированию по сети
- Не требуют объекта-носителя
- Выполняют вредоносные действия
- Используют огромное количество способов распространения

Характеристики вредоносных программ

- Целевая среда
- Объект-носитель
- Механизм передачи
- Вредоносные действия
- Механизмы активации
- Механизмы защиты

Целевая среда

- Устройства
- Операционные системы
- Приложения

Объект-носитель

- Исполняемые файлы
- Скрипты
- Макросы
- Загрузочные области носителей информации

Механизмы передачи

- Съемные носители
- Общие сетевые диски
- Сканирование сети
- Одноранговые сети
- Электронная почта
- Уязвимости удаленного доступа

Вредоносные действия

- Создание лазеек
- Порча, уничтожение информации
- Хищение данных
- Отказы в обслуживании (DoS), в т.ч. Распределенные отказы в обслуживании (DDoS)
  - Завершение системы
  - Отключение служб
  - Переполнение каналов связи

Механизмы активации

- Ручной, в т.ч. Социальная инженерия
- Полуавтоматический
- Автоматический
- По таймеру (часовой механизм)
- По событию (логические бомбы)

Антивирусное ПО

- Защита систем от угроз, связанных с действиями вредоносных программ

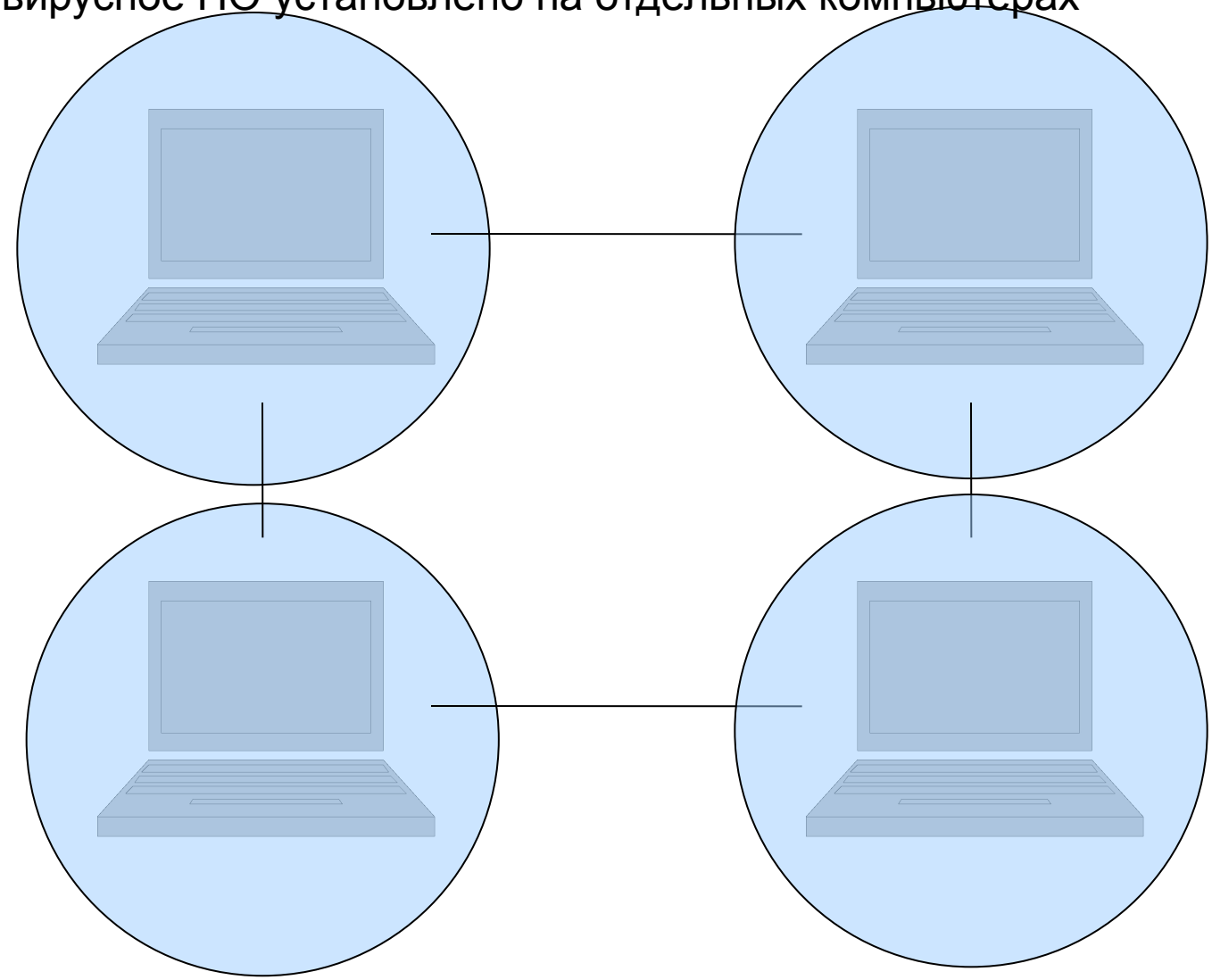
Методы работы

- Поиск сигнатур
- Эвристический анализ
- Анализ поведения

Модели организации защиты от вредоносных программ

Традиционный подход

Антивирусное ПО установлено на отдельных компьютерах



Многоуровневые системы защиты

- Выделяется несколько уровней защиты
- Для того, чтобы сработал уровень *k,* необходимо, чтобы вредоносная программа преодолела уровни защиты с 1 по *k*-1

Этапы формирования МСЗ

- оценка рисков, связанных с угрозами от ВП;
- определение уровней защиты;
- проработка углубленной модели защиты;
- формирование требований к защите отдельных уровней;
- реализация сформулированных ранее требований на практике

Оценка рисков

- Определение векторов угроз;
- Анализ средств защиты, используемых на каждом из векторов;
- Анализ степени защищенности.

Векторы угроз

- внешние сети;
- гостевые клиенты;
- мобильные клиенты;
- исполняемые файлы;
- документы;
- электронная почта;
- съемные носители информации;
- различные диски и дискеты;
- флэш-накопители.

Уровни защиты

- данные;
- приложения;
- узлы;
- внутренняя сеть;
- демилитаризованная зона;
- уровень физической безопасности

Многоуровневая система защиты

Защита клиента

- уменьшение числа уязвимых мест;
- установка и настройка обновлений системы защиты
- включение МСЭ на локальном компьютере;
- установка и настройка антивирусного ПО;
- периодическая проверка с помощью сканеров уязвимости
- использование политик с наименьшим уровнем привилегий
- ограничение использования приложений

Защита сервера

- уменьшение числа уязвимых мест;
- установка и настройка обновлений системы защиты ;
- включение МСЭ;
- на локальном компьютере;
- установка и настройка антивирусного ПО;
- периодическая проверка с помощью сканеров уязвимости;
- специализированные настройки

Условия выбора антивирусного ПО для сервера

- загрузка процессора во время проверки;
- надежность АВПО;
- трудоемкость управления;
- взаимодействие приложений

Защита уровня сети

- средства обнаружения сетевого вторжения
- фильтрация на уровне приложений
- фильтрация содержимого;
- фильтрация URL-адресов;
- карантинные сети

Физическая защита

- **Безопасность здания**. Кто имеет доступ в здание?
- **Кадровая безопасность**. Насколько ограничены права доступа сотрудников?
- **Точки доступа к сети**. Кто имеет доступ к сетевому оборудованию?
- **Серверы**. Кто имеет права доступа к серверам?
- **Рабочие станции**. Кто имеет права доступа к рабочим станциям?

Организационные меры

- процедуры поиска вирусов;
- процедуры обновления системы, АВПО, МСЭ;
- политики ограничения использования приложений;
- контроль за внесением изменений;
- мониторинг работы сети;
- процесс обнаружения атак;
- политика доступа в сеть с домашних компьютеров;
- политика доступа в сеть гостевых и мобильных пользователей;
- политика использования беспроводных сетей;
- информирование пользователей

Спасибо за внимание!