План-конспект для преподавателя

Анализ компьютерной информации средствами операционной системы

□ Общая информация о занятии

Дисциплина: Информационная безопасность / Системное администрирование

Тема: Анализ компьютерной информации средствами операционной системы

Тип занятия: Практическое занятие

Продолжительность: 4 академических часа (180 минут)

Форма проведения: Смешанная (лекция + практика)

□ Цели и задачи занятия

Образовательные цели:

- Изучить методы анализа системных файлов и журналов событий
- Освоить инструменты мониторинга активности пользователей
- Научиться создавать отчеты по результатам анализа
- Развить навыки работы с командной строкой Windows и Linux

Развивающие цели:

- Развить аналитическое мышление при работе с системными данными
- Сформировать навыки систематизации и визуализации информации
- Развить умение работать с большими объемами данных

Воспитательные цели:

- Воспитать ответственное отношение к информационной безопасности
- Сформировать понимание важности мониторинга системных событий
- Развить профессиональную этику при работе с конфиденциальными данными

□ Планируемые результаты обучения

После завершения занятия студенты должны:

Знать:

- Основные команды для анализа системных событий в Windows и Linux
- Структуру журналов событий и системных файлов
- Методы выявления подозрительной активности
- Принципы создания отчетов по результатам анализа

Уметь:

- Анализировать активность пользователей в системе
- Мониторить процессы и сетевые соединения
- Экспортировать данные в формате CSV
- Создавать графики и диаграммы в Excel
- Выявлять аномалии в работе системы

Владеть:

- Навыками работы с PowerShell и Bash
- Методами системного мониторинга
- Техниками визуализации данных
- Приемами создания технических отчетов

□ Структура занятия

1. Организационный момент (10 минут)

- Проверка присутствующих
- Объявление темы и целей занятия
- Проверка готовности рабочих мест

2. Актуализация знаний (15 минут)

Вопросы для повторения:

- Что такое журналы событий операционной системы?
- Какие типы системных событий вы знаете?
- Зачем нужен мониторинг активности пользователей?
- Какие угрозы безопасности можно выявить через анализ системных данных?

3. Изучение нового материала (30 минут)

3.1 Теоретическая часть (15 минут)

- **Типы системных событий:**
  - События входа/выхода пользователей
  - События запуска/завершения процессов

    - Сетевые события
    - События безопасности

- **Инструменты анализа:**

    - Windows: Event Viewer, PowerShell, Performance Monitor
    - Linux: journalctl, ps, netstat, ss, lsof

- **Методы выявления аномалий:**

    - Анализ временных паттернов
    - Выявление необычной активности
    - Корреляция событий

3.2 Демонстрация (15 минут)

Преподаватель демонстрирует:

1. Открытие интерактивного руководства
2. Выполнение базовых команд анализа
3. Экспорт данных в CSV
4. Создание простого графика в Excel

4. Практическая работа (110 минут)

4.1 Подготовка к работе (10 минут)

- Открытие интерактивного руководства
- Проверка прав администратора
- Создание рабочих папок

4.2 Задание 1: Анализ активности пользователей (25 минут)

Для Windows:

```
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4624,4625}
```

Для Linux:

```
last -n 50
lastb -n 20
```

Что должны найти студенты:

- Время входов и выходов пользователей

- Неудачные попытки входа
- Паттерны рабочего времени

4.3 Задание 2: Анализ процессов (25 минут)

Для Windows:

```
Get-Process | Sort-Object WorkingSet -Descending
```

Для Linux:

```
ps aux --sort=-%cpu
htop
```

Что должны найти студенты:

- Процессы с высоким потреблением ресурсов
- Подозрительные процессы
- Процессы, запущенные пользователями

4.4 Задание 3: Анализ сетевых соединений (25 минут)

Для Windows:

```
Get-NetTCPConnection
```

Для Linux:

```
ss -tulpn
lsof -i
```

Что должны найти студенты:

- Активные сетевые соединения
- Открытые порты
- Внешние соединения

4.5 Задание 4: Создание отчета в Excel (35 минут)

Студенты следуют пошаговой инструкции:

1. Импорт CSV данных

2. Создание сводных таблиц
3. Построение графиков
4. Оформление дашборда

5. Контроль и оценка (10 минут)

- Проверка выполненных заданий
- Обсуждение результатов
- Ответы на вопросы

6. Подведение итогов (5 минут)

- Резюме изученного материала
- Домашнее задание
- Объявление темы следующего занятия

□ Методические рекомендации

Подготовка к занятию:

1. **Техническая подготовка:**
    - Убедиться, что на всех компьютерах есть права администратора
    - Проверить наличие Excel или LibreOffice Calc
    - Подготовить тестовые данные для анализа
2. **Методическая подготовка:**
    - Изучить интерактивное руководство
    - Подготовить примеры подозрительной активности
    - Создать шаблоны отчетов

Во время занятия:

1. **Индивидуальный подход:**
    - Помогать студентам с разным уровнем подготовки
    - Давать дополнительные задания продвинутым студентам
    - Обеспечивать поддержку начинающим
2. **Практические советы:**
    - Поощрять эксперименты с командами
    - Объяснять практическое применение каждого инструмента
    - Показывать реальные примеры инцидентов безопасности

Работа с интерактивным руководством:

- Объяснить навигацию по разделам
- Показать функцию копирования команд
- Научить использовать чекбоксы для отслеживания прогресса

□ Критерии оценивания

Отлично (5):

- Выполнены все задания
- Созданы качественные графики в Excel
- Выявлены все аномалии в данных
- Сделаны обоснованные выводы
- Проявлена инициатива в анализе

Хорошо (4):

- Выполнено 80% заданий
- Созданы базовые графики
- Выявлена большая часть аномалий
- Сделаны корректные выводы

Удовлетворительно (3):

- Выполнено 60% заданий
- Созданы простые таблицы
- Выявлены основные проблемы
- Сделаны базовые выводы

Неудовлетворительно (2):

- Выполнено менее 60% заданий
- Не созданы отчеты
- Не выявлены аномалии
- Отсутствуют выводы

□ Домашнее задание

1. **Практическое задание:**
    - Провести анализ собственного компьютера
    - Создать отчет с графиками в Excel
    - Выявить 3 потенциальные проблемы безопасности
2. **Теоретическое задание:**
    - Изучить дополнительные команды для анализа
    - Подготовить презентацию об одном из инструментов мониторинга

□ Дополнительные материалы

Для углубленного изучения:

- Microsoft Documentation: Windows Event Logs
- Linux man pages: ps, netstat, ss, lsof
- NIST Cybersecurity Framework
- SANS Digital Forensics guides

Полезные ресурсы:

- PowerShell Gallery
- Linux Command Line tutorials
- Excel advanced charting techniques
- Cybersecurity incident response procedures

⚠ Возможные трудности и их решения

Технические проблемы:

1. **Отсутствие прав администратора:**
    - Подготовить виртуальные машины
    - Использовать демонстрационные данные
2. **Различия в версиях ОС:**
    - Подготовить альтернативные команды
    - Показать адаптацию под разные версии
3. **Проблемы с Excel:**
    - Использовать LibreOffice Calc как альтернативу
    - Подготовить онлайн-инструменты визуализации

Методические проблемы:

1. **Разный уровень подготовки студентов:**
    - Подготовить задания разной сложности
    - Организовать работу в парах
2. **Недостаток времени:**
    - Приоритизировать ключевые навыки
    - Перенести часть заданий на самостоятельную работу

□ Рефлексия и улучшения

Вопросы для анализа занятия:

- Достигнуты ли поставленные цели?
- Какие задания вызвали наибольшие трудности?
- Эффективно ли использовалось время?
- Какие методы работали лучше всего?

Предложения по улучшению:

- Добавить больше практических примеров
- Создать видео-инструкции для сложных команд
- Разработать систему автоматической проверки заданий
- Подготовить дополнительные кейсы для анализа