

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ**

Государственное образовательное учреждение высшего профессионального образования  
«Уральский государственный университет им. А.М. Горького»

ИОНЦ «Информационная безопасность»

математико-механический факультет

кафедра алгебры и дискретной математики

**УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС**

**Противодействие созданию и распространению  
вредоносных программ**

---

**Вопросы к экзамену**

Автор: доцент кафедры алгебры  
и дискретной математики В.В. Бакланов

Екатеринбург  
2008

**Теоретические вопросы:**

1. Источники образования информационного технологического «мусора» в приложениях офисного пакета (на примере Microsoft Word).
2. Событийные процедуры в VBA и их использование в компьютерных программах вредоносного и защитного назначения. Места размещения событийных процедур, их приоритет при запуске.
3. Вредоносный программный код документов офисных приложений и его возможности. Методы вирусного копирования.
4. Реализация защиты от вредоносного программного кода в приложениях офисного пакета.
5. Механизм сетевых атак на Интернет-браузеры (на примере Internet Explorer).
6. Основные настройки браузеров и почтовых клиентов, рекомендуемые при работе в Интернет. Объяснить назначение настроек исходя из реальных угроз безопасности.
7. Механизмы статического скрывания вредоносного программного кода.
8. Механизмы скрытности вредоносных программ на этапе выполнения.
9. Механизмы скрывания, используемые современными макровирусами.
10. Классификация и основные особенности различных видов вредоносных программ.
11. Способы подготовки вредоносных программ к безусловному запуску.
12. Несанкционированный характер запуска вредоносных программ.
13. Внедрение и запуск вредоносных программ на этапах самотестирования компьютера и загрузки операционной системы.
14. Способы автоматического запуска вредоносных программ.
15. Внедрение и запуск опасных команд с помощью ярлыков.

16. Способы внедрения и запуска вредоносного программного кода на клиентском компьютере с использованием Web-технологий.
17. Возможности программных закладок. Виды и способы программного перехвата компьютерной информации.
18. Виды компьютерных инфекций. Сущность вирусного заражения и жизненный цикл компьютерного вируса.
19. Возможности и особенности сетевых вредоносных программ.
20. Понятие о «троянских» программах и их функциях. Программы-«джойнеры».
21. Виды несанкционированного копирования компьютерной информации.
22. Виды нарушений работы ЭВМ со стороны вредоносных программ.
23. Виды несанкционированного блокирования и модификации компьютерной информации вредоносными программами.
24. Традиционные способы антивирусной защиты и сравнительная оценка их эффективности.

### **Практические вопросы:**

1. Статически исследовать интерпретируемый код вредоносной программы (используемые языки программирования – язык командных интерпретаторов Command.com и Cmd.exe, язык VBS с объектами и методами WSH, язык VBA). Письменно объяснить, что делает данная программа, расставить построчные комментарии. У каждого экзаменуемого – свой вариант задания.
2. Найти произвольный гипертекстовый документ, имеющий теги <OBJECT>. Используя редактор реестра и браузер объектов из составе VBE определить, какой из файлов является сервером автоматизации, и не содержит ли он опасных свойств и методов.
3. Создайте в Word документ и несколько разных шаблонов с событийными процедурами AutoOpen() и Document\_Open(). Определите и продемонстрируйте приоритеты в выполнении этих процедур. Как учесть эти приоритеты при построении антивирусной защиты?

4. Напишите текст макроса, обеспечивающего гарантированное обнаружение и отключение опасных процедур в каждом открываемом документе при отключенной защите от вирусов в макросах.
5. Продемонстрировать возможности программ-джойнеров по созданию «троянских» оболочек.