

# Лекция 15

## Особенности реализации системы безопасности в ОС Windows

### Практическое задание по лекции

**Прочитайте учебный материал лекции. Сформулируйте самостоятельно 10-15 вопросов по содержанию лекции.**

1. Какая комбинация клавиш инициирует процедуру аутентификации пользователя в системе?
2. Что такое SAS (secure attention sequence)?
3. Какая программа управляет процедурой аутентификации пользователя в системе?
4. Что происходит после успешной аутентификации пользователя в системе?
5. Какие действия доступны пользователю после нажатия комбинации клавиш "ctrl-alt-del" во время работы в системе?
6. Как можно назначить право входа в систему (SeInteractiveLogonRight) для новой учетной записи?
7. Каким образом можно включить нужные события в список проверки аудита?
8. Как можно проверить журнал событий безопасности для просмотра регистрируемых действий?
9. Какие средства защиты файлов встроены в операционную систему Windows для защиты от внешнего навязывания?
10. Как система в ОС Windows реагирует на попытку удаления системного файла?
11. Какой инструмент можно использовать для проверки корректности версии системных файлов?
12. Как создается и связывается маркер доступа с процессом-оболочкой Windows Explorer? Как можно считывать информацию о привилегиях пользователя из маркера доступа?
13. Какие возможности предоставляет функция AdjustTokenPrivileges при включении?

14. Что такое перевоплощение (impersonation) в контексте операционной системы Windows?
15. Как можно создать маркер доступа с нужным уровнем перевоплощения для указанной учетной записи?