

## ПРОГРАММА КУРСА

### «Эксплуатация системы защиты «Страж NT» (версия 3.0)»

Курс предназначен для обучения специалистов квалифицированной установке, настройке и администрированию системы защиты информации «Страж NT» (версия 3.0). В курсе рассматриваются защитные механизмы системы защиты, возможности администрирования, а также дополнительные утилиты.

Значительная часть курса уделяется практическим занятиям слушателей на специально оборудованных стендах. В процессе обучения подробно разбираются ситуации, возникающие в процессе внедрения и функционирования СЗИ, а также действия в случае возникновения нестандартных ситуаций.

#### Продолжительность курса

2 дня (12 часов)

#### Аудитория

- Специалисты, ответственные за разработку и внедрение систем информационной безопасности.
- Системные администраторы, администраторы информационной безопасности.

#### Предварительная подготовка

- Базовые понятия об организационных и технических аспектах проблемы защиты информации от несанкционированного доступа.
- Навыки установки и настройки программного обеспечения в среде MS Windows.
- Навыки администрирования локальных сетей в среде MS Windows и Active Directory.

#### По окончании обучения

- Вы приобретете знания о составе компонентов и защитных механизмах СЗИ «Страж NT» (версия 3.0).
- Вы сможете устанавливать и настраивать СЗИ «Страж NT» (версия 3.0).
- Вы сможете выполнять задачи по администрированию СЗИ «Страж NT» (версия 3.0).
- Вы сможете правильно действовать при возникновении нестандартных ситуаций.

#### Дополнительно

По окончании курса слушатель получает Сертификат об обучении. Слушатели имеют право получать консультации у специалистов в рамках пройденного курса.

#### Программа курса

##### Введение

Организация курса. Назначение СЗИ. Условия применения.

##### Структура и состав компонентов СЗИ

Подсистемы СЗИ. Описание модулей СЗИ. Варианты применения.

### **Установка и снятие СЗИ**

Подготовка к установке СЗИ. Тестирование подсистемы идентификации. Установка СЗИ. Первичный вход в систему. Программа настройки. Снятие СЗИ. Нештатные ситуации.

### **Управление пользователями**

Домены и пользователи. Свойства пользователей. Смена паролей. Формирование персональных идентификаторов. Работа с идентификаторами.

### **Менеджер файлов**

Файловые операции. Работа с защищаемыми ресурсами.

### **Замкнутая программная среда**

Основные понятия. Настройка замкнутой программной среды. Режим автозапуска. Внесение изменений и обновление ПО.

### **Избирательное управление разграничением доступа пользователей к ресурсам**

Дискреционный принцип контроля доступа. Списки управления доступом.

### **Полномочное управление разграничением доступа пользователей к ресурсам**

Основные понятия. Метки конфиденциальности. Настройка приложений для работы с грифованными ресурсами. Контроль потоков информации.

### **Управление носителями информации**

Основные понятия. Работа с группами носителей. Работа с носителями. Экспорт настроек.

### **Контроль устройств**

Группы устройств и их свойства. Экспорт настроек.

### **Целостность ресурсов**

Настройка контроля целостности ресурсов. Проверка целостности.

### **Аудит**

Настройка и использование механизмов дополнительного аудита.

### **Работа с журналами событий**

Журналы событий MS Windows и СЗИ. Группы событий. Фильтрация событий. Архивирование и очистка журналов. Анализ и разбор ситуаций.

### **Шаблоны настроек**

Создание и применение шаблонов настроек.

### **Тестирование механизмов системы защиты**

Программа тестирования. Отчеты о тестировании.

### **Дополнительные сведения о системе защиты**

Печать и маркировка документов. Монитор системы защиты. Преобразование информации. Очистка памяти. Удаление настроек. Повторная идентификация пользователей. Блокировка и разблокировка компьютера.

### **Нештатные ситуации**

Разрешение нестандартных ситуаций. Техническая поддержка.