Аннотация
к рабочей программе дисциплины
«Защита информационных ресурсов от внутренних угроз»

по направлению 10.03.01 «Информационная безопасность»

(профиль «Безопасность автоматизированных систем»)

Общая трудоемкость дисциплины составляет 5 зачетных единиц.(180 часов)

Форма контроля: экзамен 7 семестр.

Предполагаемые семестры: 7

Целью изучения дисциплины (модуля) является овладение студентами методами и средствами защиты информационных ресурсов от внутренних угроз.

Задачами курса являются:

- ознакомление с особенностями обеспечения информационной безопасности в корпоративных сетях;
- изучение различных способов аутентификации;
- изучение вопросов обеспечения безопасности информационных ресурсов в различных операционных системах;
- изучение протоколов защищенных каналов;
- ознакомление с технологиями межсетевого экранирования;
- изучение технологии защиты от вредоносных программ;
- ознакомление с методами управления сетевой защитой и системами комплексного управления безопасностью.

Учебная дисциплина относится к циклу Б1. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- сети и системы передачи информации;
- безопасность операционных систем;
- безопасность вычислительных сетей;
- английский язык в сфере профессиональных коммуникаций.

Знания и практические навыки, полученные в результате освоения дисциплины, используются студентами при разработке курсовых и дипломных работ, в научно-исследовательской работе.

Краткое содержание дисциплины:

Проблемы информационной безопасности, аутентификация, многоуровневая защита информационных ресурсов, система комплексного управления безопасностью КУБ.

В результате изучения дисциплины, студент должен обладать следующими профессиональными компетенциями (ПК):

ОПК-4: способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для обработки и поиска информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности.

В результате изучения дисциплины бакалавр должен:

Знать:

– принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

Уметь:

– формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;

– осуществлять меры противодействия нарушениям сетевой безопасности с

использованием различных программных и аппаратных средств защиты;

Владеть:

- навыками выявления и уничтожения компьютерных вирусов;
- методами и средствами выявления угроз безопасности автоматизированным системам;
- профессиональной терминологией в области информационной безопасности.