АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ»
по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Целью изучения дисциплины «Безопасность вычислительных сетей» является теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в вычислительных сетях.

Задачи освоения дисциплины:

изучение типовых угроз безопасности в вычислительных сетях;

изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в вычислительных сетях;

приобретение навыков настройки и эксплуатации средств обеспечения безопасности в вычислительных сетях;

овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;

овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в вычислительных сетях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Безопасность вычислительных сетей» изучается в 9 и 10 семестрах и относится к обязательной части дисциплин блока Б1.О специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Курс учебной дисциплины тесно увязан с другими учебными дисциплинами, в первую очередь с курсами «Информатика», «Языки программирования», «Технологии и методы программирования», «Организация ЭВМ и вычислительных систем», «Сети и системы передачи информации», «Безопасность операционных систем», «Основы информационной безопасности», «Администрирование сетей ЭВМ», позволяющими понять физическую сущность безопасности сетей ЭВМ.

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

знание базовых понятий в области информатики и вычислительной техники;

способность использовать нормативные правовые документы;

способность анализировать проблемы и процессы;

способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Безопасность открытых информационных систем»; «Разработка и эксплуатация защищённых автоматизированных систем»; «Инструментальные средства контроля защищенности информации»; «Сертификация средств защиты информации», а также в ходе всех видов практик.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
1	2
ОПК-12 - Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	**Знать:** основные принципы обеспечения безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем **Уметь:** применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем **Владеть:** навыками применения знаний в области безопасности вычислительных сетей, операционных систем и баз данных
ОПК-13 - Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	**Знать:** порядок диагностики и тестирования систем защиты информации автоматизированных систем **Уметь:** организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем **Владеть:** навыками организации и проведения диагностики и тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем
ОПК-15 - Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	**Знать:** порядок администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем **Уметь:** осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем **Владеть:** навыками администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем, инструментального мониторинга защищенности автоматизированных систем

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 11 зачетных единиц (396 часов).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии: лекционные занятия, интерактивный опрос в ходе лекций, эвристическая беседа, диалог, ознакомительные беседы с представителями потенциальных работодателей.

При организации самостоятельной работы занятий используются образовательные технологии развивающего, проблемного и проектного обучения.

6. КОНТРОЛЬ УСПЕВАЕМОСТИ

Программой дисциплины предусмотрены следующие виды текущего контроля: письменные и устные опросы на лекциях и семинарах, отчёты на лабораторных работах, защита лабораторных и курсовой работ.

Промежуточная аттестация проводится в форме экзамена.