АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Сети и системы передачи информации
Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 8 з.е.

Форма промежуточной аттестации: дифференцированный зачет (4 семестр), экзамен (5 семестр)

Планируемые результаты освоения: ОПК-1.2

Знать:

– Принципы связи и обмен данными в локальной проводной сети;
– Уровни доступа и распределения в сети Ethernet;
– Структуру сети Интернет, принципы обмена данными между узлами в Интернет;
– Схему подключения к Интернету через поставщика услуг;
– Сетевые устройства;
– Виды, характеристики и маркировку сетевых кабелей и контактов;
– Принципы сетевой адресации, формат IP-адреса и маски подсети, типы IP-адресов и методы их получения, протокол DHCP;
– Многоуровневую модель межсетевого взаимодействия OSI и сетевые протоколы;
– Беспроводные технологии для локальных сетей;
– Основные сетевые службы, архитектуру клиент-сервер, IP-сервисы и принципы их работы, сервис электронной почты, сервис доменных имен DNS;
– Архитектуру и возможности систем Cisco IOS / Huawei VRP;
– Основные протоколы маршрутизации;
– Структуру IP-адресации в ЛВС;
– Методы трансляции адресов NAT и PAT;
– Базовые настройки маршрутизаторов;
– Базовые настройки коммутаторов;
– Механизмы резервного копирования и аварийного восстановления в сети.

Уметь:

– Проектировать и устанавливать домашнюю сеть или сеть малого предприятия, а также подключать ее к сети Интернет;
– Выполнять проверку и устранять неполадки сети и подключения к сети Интернет;
– Обеспечивать общий доступ нескольких компьютеров к сетевым ресурсам (файлам, принтерам и др.);
– Выявлять и устранять угрозы безопасности локальной компьютерной сети;
– Настраивать и проверять базовые Интернет-приложения;
– Настраивать базовые IP-сервисы при помощи графического интерфейса ОС;
– Устанавливать и настраивать устройства для подключения к сети Интернет и серверам, выполнять поиск и устранение неполадок;
– Проектировать базовую проводную инфраструктуру для поддержки сетевого трафика;
– Обеспечивать подключение к сети WAN на базе сервисов телекоммуникационных компаний;
– Выполнять адекватные процедуры восстановления при авариях и осуществлять резервирование сервера;
– Контролировать производительность сети и выявлять сбои;

– Выявлять и устранять неполадки с использованием структурированной многоуровневой процедуры.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Администрирование операционных систем
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 8 з.е.

Форма промежуточной аттестации: дифференцированный зачет (5 семестр), экзамен (6 семестр)

Планируемые результаты освоения: ОПК-1.4

знать:

- основные задачи и функции администратора ОС;
- знать типы, версии и редакции ОС Windows, Linux, Unix;
- основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности;
- знать основные команды, применяемые при администрировании ОС Windows, Linux, Unix;
- основы разработки сценариев;
- базовые задачи по обеспечению защиты ОС, вычислительных ресурсов ЭВМ и данных;
- основные электронные ресурсы по теме безопасного администрирования ОС.

уметь:

- выполнять установку и конфигурирование ОС Windows, Linux, Unix;
- выполнять задачи по управлению пользователями в ОС Windows, Linux, Unix;
- выполнять задачи по управлению запоминающими устройствами в ОС Windows, Linux, Unix;
- выполнять задачи по ограничению доступа к объектам файловой системы в ОС Windows, Linux, Unix;
- конфигурировать и администрировать основные сетевые службы в ОС Windows, Linux, Unix;
- выполнять резервное копирование и восстановление данных в ОС Windows, Linux, Unix;
- конфигурировать и обслуживать основные сервисы безопасности ОС;
- определять ресурсы, подлежащие защите;
- работать с технической литературой и специализированными электронными ресурсами.

иметь навыки:

- базового администрирования ОС Windows, Linux, Unix;
- работы в командной строке;
- написания и выполнение административных сценариев;

навыками поиска технической информации.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Дополнительные главы математики
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (5 семестр)

Планируемые результаты освоения: ОПК-3

Знать
- совокупности математических методов

Уметь
- разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;
- способен использовать математические методы, необходимые для решения задач профессиональной деятельности;

Владеть
- необходимыми математическими методами для решения задач профессиональной деятельности.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Организационное и правовое обеспечение информационной безопасности
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (5 семестр)

Планируемые результаты освоения: ОПК-5

Знать:
- содержание основных понятий по правовому обеспечению информационной безопасности;
- правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;
- понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;
- правила лицензирования и сертификации в области защиты информации;
- теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию;
- основные направления и методы организационной защиты информации в организациях с различными формами собственности;
- основные положения международных стандартов в области информационной безопасности.

Уметь:
- отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности;
- разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;
- анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития.

Владеть:
- умением работы с нормативно-правовыми актами;
- умением разработки нормативно-методических материалов по регламентации системы организационной защиты информации;
- навыками применения различных способов методов защиты информации по каналам утечки и от несанкционированного доступа к ней;
- навыками проектирования систем защиты информации

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Разработка и защита web-приложений
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (5 семестр)

Планируемые результаты освоения:

ОПК-7

Знать
- принципы функционирования веб-приложений;
- наиболее распространённые web-сервера, их возможности и функционал;
- механизмы обеспечения безопасности веб-приложений;
- наиболее распространенные типы уязвимостей.

Уметь
- разрабатывать основные типы веб-приложений для наиболее распространённых web-серверов;
- производить анализ защищенности веб-приложения;
- производить защиту веб-приложения;
- производить устранение основных типов угроз.

Владеть
- терминологией веб-приложений;
- навыками разработки веб-приложений;
- навыками разработки безопасных веб-приложений для различных применений.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Системы управления базами данных
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: экзамен (5 семестр)

Планируемые результаты освоения: ОПК-12

Знать:

- типологию и методологию проектирования баз данных, уметь классифицировать информационные задачи, решаемые с использованием баз данных;
- особенности моделирования и проектирования реляционных баз данных;
- о целях и средствах разработки и администрирования баз данных;

Уметь:

- применять навыки разработки баз данных на практике;

Иметь навыки:

- владения системным подходом как методологической основой проектирования информационных систем, использующих базы данных;
- владения методикой составления запросов на языке SQL.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Технологии и методы программирования
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 8 з.е.

Форма промежуточной аттестации: дифференцированный зачет (5-6 семестр)

Планируемые результаты освоения:

ОПК-7

Знать

- основные типы программного обеспечения
- основные компьютерные технологии
- основы разработки программного обеспечения в среде Delphi
- основы разработки Win32-приложений
- основы разработки сервисов Windows
- основы разработки .NET-приложений
- основы разработки приложений для Windows Scripting Host • основы разработки VBA приложений
- основы разработки WEB-приложений под управлением IIS .

Уметь

- формализовать поставленную задачу
- разрабатывать эффективные алгоритмы и программы
- корректно использовать алгоритмы и технологии
- проводить выбор типа программного обеспечения, наиболее подходящего для решения поставленной задачи .

Владеть

- программной терминологией
- терминологией ООП
- навыками программной реализации различных видов ПО
- навыками использования и разработки структур данных
- навыками анализа, оценки и способов устранения типовых угроз ПО .

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Дополнительные главы математической статистики
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (6 семестр)

Планируемые результаты освоения: ОПК-3

Знать
- совокупности математических методов

Уметь
- разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;
- способен использовать математические методы, необходимые для решения задач профессиональной деятельности;

Владеть
- необходимыми математическими методами для решения задач профессиональной деятельности.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Интернет вещей
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (6 семестр)

Планируемые результаты освоения: ОПК-11

Знать
- основные типы оборудования используемого в проектах интернета вещей
- основные типы микроконтроллеров и микрокомпьютеров интернета вещей, их особенности, достоинства и недостатки
- основы разработки программного обеспечения в среде Arduino Studio
- наиболее распространенные типы сетей интернета вещей

Уметь
- формализовать поставленную задачу
- разбивать проект на функционально независимые блоки
- корректно подбирать необходимое оборудование
- разрабатывать алгоритм работы Владеть
- терминологией Интернета Вещей
- навыками разработки решений Интернета Вещей
- навыками разработки программ (скетчей) Интернета Вещей

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Основы управления информационной безопасностью
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (6 семестр)

Планируемые результаты освоения: ОПК-1

Знать:
- основные задачи и понятия ИБ;
- основные стандарты, регламентирующие управление ИБ;
- принципы разработки процессов управления ИБ;
- подходы к интеграции СУИБ в общую систему управления предприятием

Уметь:
- анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ;
- определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
- применять процессный подход к управлению ИБ в различных сферах деятельности;
- используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;
- практически решать задачи формализации разрабатываемых процессов управления ИБ;
- разрабатывать и внедрять СУИБ и оценивать ее эффективность.

Владеть:
- терминологией и процессным подходом построения систем управления ИБ;
- навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;
- навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Электроника и схемотехника
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (6 семестр)

Планируемые результаты освоения: ОПК-4

Знать:

- терминологию и символику, используемую в электронике, методы составления и чтения основных видов электрических схем;
- основные физические понятия и принципы функционирования базовых электронных полупроводниковых компонентов в аналоговых и цифровых системах;
- основные параметры и принципы работы базовых функциональных элементов радиоэлектроники (усилителей, генераторов и т.п.);
- основные принципы работы и проектирования электронных систем;
- особенности применения аналоговых и цифровых радиоэлектронных устройств;
- основные подходы к решению практических задач, связанных с анализом сигналов в частотной области.

Уметь:

- проводить базовые теоретические и экспериментальные исследования электронного оборудования и систем;
- оценивать степень достоверности результатов, полученных с помощью экспериментальных и теоретических методов исследований;
- рассчитывать простые аналоговые и цифровые радиоэлектронные устройства;
- применять современную вычислительную технику при анализе и разработке аналоговых и цифровых электронных устройств.

Владеть:

- приемами и навыками решения конкретных задач из разных областей электроники и схемотехники;
- основными математическими методами анализа и расчета электрических цепей и сигналов;
- базовыми навыками проектирования, конструирования, монтажа и наладки простых радиоэлектронных устройств.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Защита в операционных системах
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: экзамен (7 семестр)

Планируемые результаты освоения: ОПК-1.1

знать:
- основные понятия и положения защиты информации в ОС;
- основные угрозы ИБ в ОС;
- ресурсы, подлежащие защите;
- требования к обеспечению ИБ в ОС;
- основные сервисы безопасности ОС, принципы их организации и структуру;
- методы обеспечения ИБ в ОС;
- перечень программно-технических мер ИБ в ОС;
- основные ресурсы для поиска информации об уязвимостях ОС;
- содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности;

уметь:
- проводить анализ угроз информационной безопасности в ОС;
- оценивать эффективность и надежность защиты ОС;
- находить информацию об актуальных угрозах ОС, уязвимостях ОС;
- выявлять слабые места в защите ОС;
- конфигурировать встроенные сервисы безопасности ОС;
- проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
- проводить инструментальный контроль защищенности ОС;
- самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности; иметь

навыки:
- поиска и анализа информации об уязвимостях ОС;
- анализ угроз информационной безопасности в ОС;
- безопасного администрирования ОС;
- оценки уровня безопасности ОС;
- использования средств инструментального контроля защищенности ОС.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Защита государственных информационных систем и персональных данных
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (7 семестр)

Планируемые результаты освоения: ОПК-13

Знать:

- основные понятия в области защиты государственных информационных систем и персональных данных;
- необходимость, принципы и методы защиты государственных информационных систем и персональных данных;
- основные положения НПА в области защиты государственных информационных систем и персональных данных;
- правила определения нарушителей и угроз безопасности информации;
- правила формирования перечня мер по защите информации;
- правила выбора компенсирующих мер;
- правила выбора необходимых средств защиты информации.

Уметь:

- определять уровень защищенности информационных систем персональных данных;
- моделировать угрозы и нарушителей безопасности информации в соответствии с требованиями ФСТЭК России и ФСБ России;
- формировать перечни требований и мер по защите информации;
- разрабатывать техническое задание и проект на внедрение системы защиты информации;
- осуществлять подбор средств защиты информации в зависимости от требований.

Владеть:

- навыками сбора и подготовки исходных данных об информационной системе;
- навыками использования специального ПО для создания схем в области ИБ;
- навыками определения организационной и технической реализации мер по защите информации;
- навыками анализа выбора компенсирующих мер по защите информации;
- навыками написания официальных писем и запросов юридическим лицами.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Защита информации от утечки по техническим каналам
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: экзамен (7 семестр)

Планируемые результаты освоения: ОПК-10

знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области;
- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;

уметь:

- анализировать и оценивать угрозы информационной безопасности объекта;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- пользоваться нормативными документами по защите информации;

владеть:

- навыками работы с нормативными правовыми актами;
- методами и средствами выявления угроз безопасности;
- методами технической защиты информации;
- методами формирования требований по защите информации;
- методами расчета и контроля показателей технической защиты информации;
- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- профессиональной терминологией.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Методы и средства криптографической защиты информации
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (7 семестр)

Планируемые результаты освоения: ОПК-9

знать:
- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- модели шифров и математические методы их исследования;
- принципы построения криптографических алгоритмов;
- криптографические стандарты;
- использование криптографических стандартах в информационных системах;
- о системах криптографической защиты информации (СКЗИ).

уметь:
- применять криптографические алгоритмы на практике;
- применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- осуществлять программную реализацию криптографических алгоритмов;
- пользоваться научно-технической литературой в области криптографии;

владеть:

- криптографической терминологией;
- навыками программной реализации криптографических алгоритмов;
- навыками использования типовых криптографических алгоритмов;
- навыками использования ПЭВМ в анализе простейших шифров;
- навыками математического моделирования в криптографии;
- средствами обеспечения информационной безопасности;
- навыками определения видов и форм информации, подверженных угрозам и возможных методов и путей устранения этих угроз.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Методы оценки безопасности компьютерных систем и сетей (пентестинг)
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (7 семестр)

Планируемые результаты освоения: ОПК-2

Знать:
- различные подходы к организации процесса проверки подлинности сущностей информационной безопасности;
- особенности моделей разграничения прав доступа в информационной системе;
- способы учитывать и анализировать действия пользователей в информационной системе;
- методики проведения аудита информационной безопасности и теста на проникновение;

Уметь:
- реализовывать различные методы проверки подлинности сущностей информационной безопасности;
- адекватно применять ту или иную модель разграничения прав доступа;
- учитывать и анализировать действия пользователей в информационной системе программными методами;
- проводить аудит информационной безопасности и тест на проникновение;

Владеть:
- навыками реализации различных подходов к проверке подлинности сущностей информационной безопасности;
- навыками адекватного применения и реализации различных моделей разграничения прав доступа;
- навыками построения системы учета и анализа действия пользователей в информационной системе;
- навыками организации и проведения аудита информационной безопасности и теста на проникновение.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Основы построения защищенных баз данных
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (7 семестр)

Планируемые результаты освоения: ОПК-1.3

знать:
- сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
- средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- современные критерии и стандарты для анализа безопасности информационных систем на базе СУБД;
- нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, предоставляемые системами управления базами данных;
- принципы построения систем защиты информации;

уметь:
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять действующую законодательную базу в области обеспечения безопасности систем баз данных;
- применять отечественные и зарубежные стандарты для проектирования, разработки и оценивания защищенности компьютерной системы;
- формализовать поставленную задачу по обеспечению защиты БД;
- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- использовать средства защиты, предоставляемые системами управления базами данных;
- проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований;

владеть:
- методиками использования средств защиты, предоставляемых системами управления базами данных;
- профессиональной терминологией в области информационной безопасности;
- практическими навыками работы с научно-технической документацией;
- навыками разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;
- навыками разработки модели угроз и модели нарушителя безопасности компьютерных систем;
- навыками разработки частных политик безопасности, в том числе политик управления доступом и информационными потоками;

- методами анализа безопасности информационных систем на базе промышленных СУБД;
- навыками формирования требований по защите информации.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации подготовки: Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (7 семестр)

Планируемые результаты освоения: ОПК-6

Знать:

- методы защиты компьютерной информации;
- классификацию и общую характеристику программно-аппаратных средств защиты информации;
- основные принципы администрирования защищенных компьютерных систем;
- особенности реализации методов защиты информации программно-аппаратными средствами;

Уметь:

- выполнять функции администратора безопасности защищенных компьютерных систем;
- выполнять настройку защитных механизмов программно-аппаратных средств;
- настраивать политику безопасности средствами программно-аппаратных комплексов защиты информации;
- применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных систем;
- выполнять защиту рабочих мест с использованием программно-аппаратных средств защиты информации;

Владеть:

- средствами администрирования программно-аппаратных комплексов защиты информации от несанкционированного доступа;
- средствами администрирования комплексов криптографической защиты информации;
- средствами контроля и анализа защищенности.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Научно-проектный (исследовательский) семинар
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (8 семестр)

Планируемые результаты освоения: ОПК-8,УК-1,2,3,4,5,9

знать:

- правила оформления отчета по курсовой работе;
- правила оформления списка литературы;
- основные научные проблемы в области ИБ;

уметь:

- применять методы научных исследований в профессиональной деятельности;
- осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности;

владеть:

- навыками проведения научно-исследовательской работы;
- навыками разработки научно-технических отчетов, обзоров, публикаций по результатам выполненных работ.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Основы построения защищенных компьютерных сетей
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: экзамен (6 семестр)

Планируемые результаты освоения: ПК-1

Знать:
- Угрозы нарушения информационной безопасности компьютерных сетей.
- Основные криптографические методы защиты информации.
- Архитектуру и функции систем управления сетями, стандарты систем управления.
- Принципы функционирования защищенных сетевых протоколов.
- Средства мониторинга и анализа компьютерных сетей.
- Методы устранения неисправностей в технических системах.

Уметь:
- Применять основные протоколы и технологии обеспечения безопасности компьютерных сетей.
- Выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств.
- Осуществлять диагностику и поиск неисправностей всех компонентов сети.
- Выполнять действия по устранению неисправностей.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Защита корпоративных сетей
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: дифференцированный зачет (7 семестр)

Планируемые результаты освоения: ПК-2,3

Знать:

- основы проектирования и работы безопасных коммутируемых сетей;
- организацию и распространение виртуальные локальные сети;
- основы безопасной маршрутизации между сегментами внутри кампусной сети;
- основы безопасности коммутируемых сетей на уровне распределения (distribution);
- основы безопасности коммутируемых сетей на уровне доступа (access);

Уметь:

- настраивать порты коммутатора для подключения WI-FI-точек доступа;
- проектировать и настраивать маршрутизацию между VLAN;
- управлять беспроводным котроллером;
- конфигурировать протоколы FHRP;
- настраивать протоколы класса Spanning Tree;
- применять технологии отказоустойчивости, высокой доступности и мониторинга безопасности компьютерных сетей.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Проектирование и внедрение систем защиты информации»
Направление подготовки: 10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единиц, 144 академических часов.

Форма промежуточной аттестации: Дифференцированный зачет (6 семестр).

Цели и задачи освоения дисциплины (модуля)

Цель дисциплины «Проектирование и внедрение систем защиты информации»: закрепление теоретических знаний и практических навыков в области построения, разработки и внедрения систем защиты информации для различных информационных систем.

Основными задачами дисциплины являются:

- изучение требований ГОСТов и НПА по проектированию СЗИ;
- изучение возможностей и освоение функционала различных инструментов по проектированию СЗИ;
- формирование требований к проектируемой системе защиты информации с учетом анализа угроз;
- разработка технического задания и технического проекта на создание системы защиты информации.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ПК-4. Способен организовывать и проводить работы по технической защите информации.

В результате изучения дисциплины студент должен:

Знать

- общие принципы построения и внедрения систем защиты информации для автоматизированных систем;
- необходимые для проектирования ГОСТы и НПА;
- принципы проектирования архитектуры, структуры и основных объектов защищаемых автоматизированных систем;
- основные этапы процесса проектирования и методы, используемые при построении проектируемой системы защиты информации.

Уметь

- формировать требования к проектируемой системе защиты информации с учетом анализа угроз;
- составлять функциональные схемы проектируемой СЗИ и АС.

Владеть

- методами построения защищенных автоматизированных систем;
- навыками составления, технического задания, технического проекта и пониманием содержания основных этапов процесса проектирования.

Краткое содержание дисциплины (модуля)

Дисциплина включает 6 тем:

Тема 1. Основные термины и понятия дисциплины.

Тема 2. Этапы проектирования СЗИ

Тема 3. Определение требований к СЗИ
Тема 4. ГОСТы по разработки и проектированию СЗИ
Тема 5. Инструментарий по проектированию СЗИ
Тема 6. Разработка технического задания и технического проекта на создание СЗИ