МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Администрирование операционных систем»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 7 зачетных единиц,.252 академических часа.

Форма промежуточной аттестации: экзамен.

Цели и задачи освоения дисциплины (модуля)

Учебная дисциплина «Администрирование операционных систем» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Администрирование операционных систем» является изложение основополагающих принципов администрирования операционных систем (ОС) и примеров реализации подобных методов на практике.

Задачи дисциплины «Администрирование операционных систем»:

- дать представление об основных задачах администрирования ОС и методах их решения;
- научить использовать встроенные средства ОС для решения задач администрирования ОС.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8 - способность к самоорганизации и самообразованию;

ОПК-7: способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ПК-8: способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы;

ПК-15: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы;

ПК-17: способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение;

ПК-18: способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

В результате изучения дисциплины студент должен:

знать:

- основные задачи и функции администратора ОС;
- типы, версии и редакции ОС Windows, Linux, Unix;
- основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности;
- 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;
- содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности;

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;
- самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности.

Краткое содержание дисциплины (модуля)

Тема 1. Введение в администрирование ОС.
Тема 2. Базовые инструменты администрирования ОС Windows.
Тема 3.Управление локальными пользователями в ОС Windows.
Тема 4. Управление дисковыми ресурсами.
Тема 5. Сетевые параметры в ОС Windows.
Тема 6. Система доменных имен.
Тема 7. Протокол динамической конфигурации хоста.
Тема 8. Настройка файлового сервера под управлением ОС Windows.
Тема 9. Администрирование доменов в сетях Windows.
Тема 10. Настройка удаленного доступа в Windows.
Тема 11. Резервное копирование данных.
Тема 12. Мониторинг работы и контроль производительности ОС Windows.
Тема 13. Автоматизация задач администрирования в ОС Windows. PowerShell.
Тема 14. Общий обзор Unix-like систем. ОС FreeBSD.
Тема 15. Командная строка FreeBSD.
Тема 16. Управление локальными пользователями в ОС FreeBSD.
Тема 17. Управление дисковыми ресурсами, ФС UFS.
Тема 18. Ограничение доступа к файлам и каталогам.
Тема 19. Сетевые параметры в ОС FreeBSD.
Тема 20. Загрузка ОС FreeBSD. Сборка ядра, обновление системы.
Тема 21. Установка программного обеспечения в ОС FreeBSD.
Тема 22. Сервер имен под управлением ОС FreeBSD.
Тема 23. DHCP-сервера под управлением ОС FreeBSD.
Тема 24. Файловый сервер под управлением ОС FreeBSD.
Тема 25. Организация удаленного доступа к серверу под управлением ОС FreeBSD.
Тема 26. Организация резервного копирования и восстановления данных в ОС FreeBSD.

Тема 27. Мониторинг работы и контроль производительности ОС FreeBSD.
Тема 28. Обеспечение отказоустойчивости ОС FreeBSD.
По дисциплине предусмотрена курсовая работа.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Анализ и управление рисками информационной безопасности»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 5 зачетных единиц, , 180 академических часа.

Форма промежуточной аттестации: экзамен.

Цели и задачи освоения дисциплины (модуля)

Анализ и управление рисками информационной безопасности обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной целью дисциплины «Анализ и управление рисками информационной безопасности» является изучение методов и средств управления информационной безопасностью (ИБ) на объекте информатизации, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта (СУИБ).

Задачи дисциплины:

- познакомить студентов с основными терминами и определениями из области оценки и анализа рисков информационной безопасности;
- обучить методикам оценки и анализа рисков информационной безопасности;
- сформировать навыки построения системы управления информационной безопасностью;
- сформировать навыки построения системы управления информационными рисками.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8: способностью к самоорганизации и самообразованию;

ПК-7: способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем;

В результате изучения дисциплины студент должен:

знать:

- нормативные акты и стандарты в области управления рисками информационной безопасности;
- основные определения и термины из области оценки и анализа рисков информационной безопасности;
- методики оценки и анализа рисков информационной безопасности;
- методики разработки политики информационной безопасности;
- принципы построения и сопровождения системы управления информационным рисками и системы управления информационной безопасностью;

умеет:

- определять субъекты и объекты информационной системы;

- составлять модель угроз и модель злоумышленника;
- разрабатывать политику информационной безопасности;
- оценивать и анализировать риски информационной безопасности;
- внедрять и сопровождать систему управления информационным рисками и систему управления информационной безопасностью;

Краткое содержание дисциплины (модуля)

Тема 1. Определения риска информационной безопасности. Обзор различных подходов к анализу рисков информационной безопасности.
Тема 2. Методики расчёта величины риска информационной безопасности.
Тема 3. Управление рисками информационной безопасности.
Тема 4. Процессный подход. Цикл ДемингаШухарта.
Тема 5. Обзор серий стандартов BS 7799, ISO 27000.
Тема 6. Минимизация, ликвидация, принятие и делегирование рисков информационной безопасности
Тема 7. Определение и структура системы управления информационными рисками.
Тема 8. Система управления информационными рисками как фундамент системы управления информационной безопасностью.
Тема 9. Выбор и обоснование контрмер для повышения уровня защищённости информационной системы.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Аудит информационной безопасности»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 3 зачетные единицы.

Форма промежуточной аттестации: зачет.

Цели и задачи освоения дисциплины (модуля)

Аудит информационной безопасности направлена на освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе организации и проведения аудита информационной безопасности.

Цель дисциплины «Аудит информационной безопасности» - изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта (СУИБ). Приобретенные знания позволят студентам основывать свою профессиональную деятельность на процессном подходе, формировать требования к системе управления ИБ конкретного объекта, принимать участие в проектировании системы управления ИБ, принимать участие в эксплуатации системы управления ИБ.

Задачи курса - изучение:

формирования требований к системе управления ИБ конкретного объекта;

проектирование системы управления ИБ конкретного объекта;

эффективное управление ИБ конкретного объекта.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-7: способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ПК-10: способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

В результате изучения дисциплины студент должен:

Знать:

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;

- принципы организации информационных систем в соответствии с требованиями по защите информации.
-

Уметь:

- составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;
- выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах.

Краткое содержание дисциплины (модуля)

Модуль 1.
Тема 1. Базовые вопросы управления ИБ.
Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Стандартизация в области построения систем управления. История развития.
Тема 2. Процессный подход.
Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода.
Тема 3. Область деятельности СУИБ.
Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры).
Тема 4. Ролевая структура СУИБ.
Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли).
Тема 5. Политика СУИБ.
Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ.
Тема 6. Рискология ИБ.
Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов.
Модуль 2.
Тема 7. Основные процессы СУИБ.
Обязательная документация СУИБ Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ).
Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».
Тема 8. Внедрение разработанных процессов.
Документ «Положение о применимости» Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБ, и способы их решения. Контроль над внедрением процессов.
Тема 9. Процесс «Управление инцидентами ИБ».
Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ. Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.
Тема 10. Процесс «Обеспечение непрерывности ведения бизнеса».

Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.

Модуль 3.

Тема 11. Обеспечение соответствия требованиям законодательства РФ.

Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.).

Тема 12. Эксплуатация и независимый аудит СУИБ.

Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.

Тема 13. Программные средства аудита ИБ.

Проведение анализа рисков информационной безопасности. Моделирование угроз информационной безопасности и уязвимостей. Разработка и управление политикой безопасности ИС.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Введение в теорию вероятностей и математическую статистику»
Специальность 10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения - очная

Трудоемкость дисциплины: 3 зачетных единиц, 108 академических часов.

Форма промежуточной аттестации: 3 семестр - экзамен.

Цели и задачи освоения дисциплины

Целью изучения данной дисциплины является знакомство студентов с основными понятиями, методами и результатами теории вероятностей и математической статистики. Объектами изучения в данной дисциплине являются случайные события и случайные величины. С их помощью могут быть сформулированы как законы природы, так и разнообразные процессы, происходящие в экономике, природе, технике. Отсюда объективная важность теории вероятностей и математической статистики как средства изучения случайных явлений и процессов. Задачами является изучение различных вероятностных моделей случайных событий, свойств распределений случайных величин, предельных теорем, основных задач математической статистики. Большое внимание уделяется вопросам построения математических моделей случайных экспериментов, проверке статистических гипотез, выявлению взаимосвязей между исследуемыми признаками и выработке навыков применения изученных методов при решении практических задач.

Планируемые результаты освоения

Код и наименование компетенции (из ФГОС ВО)	Компонент (знаниевый/функциональный)
Способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов. (ОПК-2)	Знает основные понятия, теоремы и методы алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, использующихся при изучении общетеоретических и специальных дисциплин учебного цикла; Умеет использовать знания фундаментальных основ, подходы и методы математики при решении прикладных задач; пользоваться источниками для самостоятельного изучения специальной литературы;
Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности	Знает: основные приемы решения задач обработки текстовой и числовой информации; основные способы и принципы представления структур данных;

информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований. (ПК-2)	Умеет: выполнять основные этапы реализации программ на компьютере; реализовывать подходы процедурного программирования, реализацию вызова процедур в языках с блочной структурой.
Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем. (ПК-4)	Знает: угрозы информационной безопасности информации и модели нарушителя в АС, криптографические, программно-аппаратные и технические средства и методы защиты АС; Умеет: разрабатывать и исследовать АС

Краткое содержание дисциплины

Введение в теорию вероятностей и математическую статистику. Основные понятия теории вероятностей. Случайные события. Классическое, геометрическое, статистическое и аксиоматическое определения вероятности события. Условная вероятность. Теоремы сложения и умножения вероятностей. Формула полной вероятности. Формула Байеса. Схема Бернулли. Случайные величины. Дискретные случайные величины. Непрерывные случайные величины. Примеры распределений известных случайных величин.

Законы распределения. Числовые характеристики случайных величин. Закон больших чисел. Центральная предельная теорема. Генеральная совокупность. Выборки. Основные выборочные характеристики. Статистические оценки. Методы статистического оценивания. Статистическая проверка гипотез.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Защита операционных систем»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 7 зачетных единиц, 252 академических часа.

Форма промежуточной аттестации: зачет (7 семестр), экзамен (8 семестр).

Цели и задачи освоения дисциплины (модуля)

Учебная дисциплина «Защита операционных систем» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Защита операционных систем» является изложение основополагающих принципов защиты операционных систем (ОС) и примеров реализации подобных методов на практике.

Задачи дисциплины «Защита операционных систем»:

- дать представление об основных угрозах ИБ для современных ОС;
- научить оценивать уровень защищенности ОС с учетом актуальных моделей угроз и требований руководящих документов;
- дать основы системного подхода к обеспечению безопасности в современных ОС;
- изучить сервисы безопасности современных ОС и научить использовать их для защиты ОС.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-7: способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ОПК-9: способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации;

ПК-5: способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической;

ПК-8: способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы;

ПК-15: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы;

ПК-17: способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение;

ПК-18: способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления

базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
ПСК-3.2: способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем.

В результате изучения дисциплины студент должен:
знать:

- основные понятия и положения защиты информации в ОС;
- основные угрозы ИБ в ОС;
- ресурсы, подлежащие защите;
- основные понятия программно-технического уровня ИБ;
- 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;

уметь:

- проводить анализ угроз информационной безопасности в ОС;
- проводить классификацию возможных угроз ИБ 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.

Краткое содержание дисциплины (модуля)
Тема 1. Основные понятия и положения защиты информации в АС.
Тема 2. Угрозы ИБ: определения, анализ и классификация.
Тема 3. Основные направления и методы реализации угроз ИБ.
Тема 4. Программно-технические меры ИБ, сервисы ИБ.
Тема 5. Требования безопасности информации к операционным системам
Тема 6. Модели безопасности основных операционных систем.
Тема 7. Базовые сервисы безопасности ОС Windows. Реализация, конфигурирование, уязвимости, компрометация, защита.
Тема 8. Дополнительные механизмы защиты в ОС Windows.
Тема 9. Организация защищенного удаленного доступа в ОС Windows.
Тема 10. Сетевая безопасность в ОС Windows.
Тема 11. Аудит безопасности в ОС Windows.
Тема 12. Базовые сервисы безопасности в Unix-like систем. Реализация, конфигурирование, уязвимости, компрометация, защита.
Тема 13. Дополнительные механизмы защиты объектов ФС в Unix-like системах.
Тема 14. Шифрование, контроль целостности в Unix-like системах.
Тема 15. Мандатная модель управления доступом в Unix-like системах.
Тема 16. Подключаемые модули аутентификации.
Тема 17. Организация защищенного удаленного доступа в Unix-like системах.
Тема 18. Сетевая безопасность в Unix-like системах.
Тема 19. Аудит безопасности в Unix-like системах.
Тема 20. Общие рекомендации по защите ОС.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Защита программ и данных»
Направление подготовки:
10.05.01 «Компьютерная безопасность (специалитет)»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единиц.

Форма промежуточной аттестации: экзамен.

Цели и задачи освоения дисциплины (модуля)

− Цель дисциплины «Защита программ и данных» является изучение программных способов и методов защиты современных сетевых сервисов и протоколов маршрутизации, а также - изучение основных подходов к эксплуатации технологий защиты при передаче информации в сети предприятия.

Задачи курса:

− Анализ принципов функционирования и защиты современных протоколов маршрутизации в сети предприятия;
− Организация безопасных базовых сервисов в сети предприятия средствами современного телекоммуникационного оборудования;
− Изучение функциональных возможностей современных технологий защиты передачи информации в сети предприятия.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-8 - способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач.

В результате изучения дисциплины студент должен:
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.

Краткое содержание дисциплины (модуля)
Дисциплина включает 9 тем:
Тема 1. Защита программ и данных в компьютерной сети
Тема 2. Маршрутизация в сети предприятия
Тема 3. Статические маршруты для IPv4 / IPv6
Тема 4 Защита протокола RIP.
Тема 5 Защита протокола EIGRP.
Тема 6. Защита протокола OSPF.
Тема 7. Подключение сети предприятия к сети Интернет с использованием протокола BGP.
Тема 8. Защита основных сервисов сети предприятия
Тема 9. Защита передаваемых по сети данных.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

ИНТЕРНЕТ ВЕЩЕЙ

10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 3 зачетных единиц.
Форма промежуточной аттестации: зачет(6 семестр).
Цели и задачи освоения дисциплины (модуля)

Цели и задачи дисциплины

Цель дисциплины: сформировать навыки разработки и анализа проектов интернета вещей при решении разнообразных прикладных задач.

Задачи дисциплины:

- сформировать понимание принципов разработки и функционирования сенсоров и установок IoT;
- развить навыки использования сенсоров IoT и разработки устройств IOT.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
ОПК-7 - способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения.

В результате изучения дисциплины студент должен:
знать:

- архитектуру устройств ИВ и особенности сенсоров ИВ..

уметь:

- разрабатывать устройства ИВ с учётом особенностей сенсоров ИВ и их взаимодействия с современными системами ИВ..

Краткое содержание дисциплины (модуля)

1. Введение в дисциплину
2. Аналоговые сенсоры
3. Сети IoT. Устройства и цифровые сенсоры.
4. Взаимодействие с Интернет

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«История создания технологий хранения, передачи и защиты информации»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 3 зачетных единиц.
Форма промежуточной аттестации: зачет.
Цель дисциплины «История создания, хранения, передачи и защиты информации» - является изложение истории развития мировой и отечественной мысли в области коммуникаций, а также истории защиты информации в средствах коммуникации.

Задачи курса - изучение:

- основных этапов истории развития коммуникаций терминологии;
- истории аналоговой коммуникации;
- истории и тенденции развития цифровых коммуникаций;
- основных технологий цифровых коммуникаций и их защищенность.

Планируемые результаты освоения
В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-5: способностью понимать социальную значимость своей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;
ОПК-3: способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации;
ПК-3: способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности;
ПК-9: способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы;
ПК-10: способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты;
ПК-12: способностью проводить инструментальный мониторинг защищенности компьютерных систем;
ПК-17: способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение;

ПК-18: способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-19: способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации;

ПК-20: способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций;

ПСК-3.1: способность использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем;

ПСК-3.2: способность анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем;

В результате изучения дисциплины студент должен:
Знать:

- свойства информации, подлежащие закрытию;
- этапы развития средств и технологий коммуникаций;
- историю развития информационного противоборства в России и мире
- основные технологии передачи цифровой информации;
- назначение основных устройств (маршрутизаторов, коммутаторов) обеспечивающих передачу цифровой информации.
- основные стандарты, используемые при передаче цифровой информации;
- основные технологии защиты информации.

Уметь:
- ориентироваться в истории технологий передачи информации, методах защиты информации в контексте исторического развития.
- создавать и настраивать LAN сети.
- создавать, безопасное подключение LAN к Интернет.

Краткое содержание дисциплины (модуля)
Дисциплина включает 9 тем:
Тема 1. Введение в технологии защищенных коммуникаций
Тема 2. 3 этапа развития защищенных коммуникаций
Тема 3. Локальные, корпоративные и глобальные сети
Тема 4. Сетевая адресация. IP адреса и маска подсети
Тема 5. Сетевые службы
Тема 6. Беспроводные технологии
Тема 7. Основы безопасности цифровых коммуникаций
Тема 8. Структура, адресация и настройка сети. Маршрутизация
Тема 9. Коммутируемая архитектура. Корпоративные сети.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Криптографические методы защиты информации»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»

форма обучения очная

Объем дисциплины (модуля): 4 зачетные единицы.

Форма промежуточной аттестации: экзамен.

Цели и задачи освоения дисциплины (модуля)

Программа дисциплины ориентирована на достижение следующих целей: · приобретение основных знаний о методах криптографических преобразований информации и методах криптоанализа современных шифров; овладение умением чтения российских и зарубежных криптографических стандартов; · воспитание ответственности к профессиональной деятельности, воспитание самообразования; · развитие навыков программной реализации криптографических алгоритмов; · формирование готовности использовать приобретенные знания в профессиональной деятельности.

Исходя из целей, в программе дисциплины «Криптографические методы защиты информации» предусматриваются задачи: · сформировать у обучающегося необходимый объем знаний о принципах разработки шифров и методах их криптоанализа; · научить читать базовые российские и зарубежные криптографические стандарты; · развить навыки программной реализации криптографических алгоритмов; · сформировать умения применять знания о математических методах построения криптографических средств защиты информации на практике.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8 - способность к самоорганизации и самообразованию;

ПК-5 - способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-10 - способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

В результате изучения дисциплины студент должен:

Знать:

- содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования

- внутреннюю структуру криптографических алгоритмов, их область применения и свойства; внутреннее содержание отечественных криптографических стандартов, их характеристики по сравнению с зарубежными;
- основы теорий секретности и имитостойкости, тесты на простоту, общие приемы дифференциального и линейного криптоанализа, основные алгоритмы факторизации и дискретного логарифмирования. Математические модели и свойства криптосистем.

Уметь:

- самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
- самостоятельно реализовать стандартный криптографический алгоритм; применять на практике отечественные и зарубежные стандарты;
- показать полноту и корректность криптосистемы, получать криптографические ключи, построить математическую модель и вычислить вероятностные характеристики криптосистемы.

Краткое содержание дисциплины (модуля)

Дисциплина включает 10 тем:

Тема 1. Введение в криптографию

Тема 2. История криптографии. Исторические шифры.

Тема 3. Математическая модель шифра. Теория секретности Шеннона.

Тема 4. Блочные шифры

Тема 5. Псевдослучайные последовательности и поточные шифры.

Тема 6. Теория имитостойкости Симмонса и криптографические хэш-функции.

Тема 7. Асимметричные (с открытым ключом) шифры.

Тема 8. Схемы цифровой подписи

Тема 9. Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе.

Тема 10. Введение в криптографические протоколы.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Криптографические протоколы»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 3 зачетные единицы.

Форма промежуточной аттестации: зачет.

Цели и задачи освоения дисциплины (модуля)

Программа дисциплины ориентирована на достижение следующих целей: · приобретение основополагающих знаний о подходах к анализу и синтезу криптографических протоколов с государственными и международными стандартами в этой области; овладение навыками корректного применения современных защищенных информационных технологий; · воспитание ответственности к профессиональной деятельности, воспитание самообразования; · развитие навыков программной реализации криптографических протоколов; · формирование готовности использовать приобретенные знания в профессиональной деятельности.

Исходя из целей, в программе дисциплины «Криптографические протколы» предусматриваются задачи: · сформировать у обучающегося необходимый объем знаний об основных механизмах функционировая протоколов, применяемых для обеспечения того или иного свойства безопасности; · научить корректно применять современные защищенные информационные технологии; · развить навыки программной реализации криптографических протоколов; · сформировать умения применять знания о свойствах, характеризующих защищенность криптографических протоколов на практике.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8 - способность к самоорганизации и самообразованию;

ПК-8 – способность участвовать в разработке подсистемы информационной безопасности компьютерной системы;

ПК-18 – способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

В результате изучения дисциплины студент должен:

Знать:

- содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования;
- основы Интернет-технологий; средства и методы хранения и передачи аутентификационной информации; основные протоколы идентификации и аутентификации

абонентов сети;

- средства и методы хранения и передачи аутентификационной информации; основные протоколы идентификации и аутентификации абонентов сети; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; криптографические стандарты; алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах.

Уметь:

- самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
- формализовать поставленную задачу; разрабатывать эффективные алгоритмы и программы; корректно применять симметричные и асимметричные криптографические алгоритмы;
- разрабатывать эффективные алгоритмы и программы; корректно применять симметричные и асимметричные криптографические алгоритмы; проводить оценку сложности алгоритмов.

Краткое содержание дисциплины (модуля)

Дисциплина включает 9 тем:

Тема 1. Основные понятия.

Тема 2. Привязка к биту и электронная жеребьевка.

Тема 3. Разделение секрета.

Тема 4. Идентификация и аутентификация

Тема 5. Протоколы идентификации с нулевым разглашением.

Тема 6. Протоколы открытых сделок

Тема 7. Инфраструктура открытых ключей.

Тема 8. Управление ключами.

Тема 9. Прикладные протоколы.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Модели безопасности компьютерных систем»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 3 зачетные единицы.

Форма промежуточной аттестации: зачет.

Цели и задачи освоения дисциплины (модуля)

Основной целью дисциплины «Модели безопасности компьютерных систем» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации; обучение общим принципам построения моделей безопасности и политик безопасности, основным методам исследования корректности систем защиты, методологии обследования и проектирования систем защиты.

Задачи дисциплины «Модели безопасности компьютерных систем»:

· изложение теоретических основ компьютерной безопасности;

· описание моделей безопасности информационных систем;

· описание моделей доступа в информационных системах;

· обучение методологии обследования и проектирования систем защиты;

· обучение навыкам настройки основных компонентов систем защиты и применения технологий защиты.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-7 - способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности;

ОПК-10 - способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

ОПК-2 - способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов;

ОПК-4 - способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ОПК-9 - способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации;

ПК-1 - способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности;

ПК-2 - способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований;
ПК-4 - способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.

В результате изучения дисциплины студент должен:
Знать:
основные модели доступа в информационной системе;
методы формального описания модели злоумышленника;
основные способы формального описания и анализа политик безопасности;
методы анализа модели угроз.

Уметь:
реализовывать основные модели доступа в информационной системе;
формально описывать модель злоумышленника;
формально описывать и анализировать политику безопасности;
анализировать модель угроз.

Краткое содержание дисциплины (модуля)
Модуль 1. Формальное обоснование информационной безопасности информационных систем.
1. Введение в теоретический подход к обеспечению информационной безопасности. Основные понятия защиты информации (субъекты, объекты, доступ, граф доступов, информационные потоки). Постановка задачи построения защищенной автоматизированной системы (АС). Ценность информации.
2. Математические основы построения моделей безопасности. Применение теории графов и теории автоматов для обеспечения информационной безопасности информационных систем. Понятие автомата, графа, математической решѐтки. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы. Проблема адекватности реализации модели безопасности в реальной компьютерной системе.
3. Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU). Определение дискреционного контроля доступа. Принципы построения матрицы доступов. Контроль над процессом передачи прав доступа в системе. Модель системы безопасности Харрисона-РуззоУльмана (HRU). Основные положения модели. Теорема об алгоритмической неразрешимости задачи проверки безопасности произвольной системы HRU
Модуль 2. Дискреционная и мандатная модели разграничения прав доступа в информационной системе.
4. Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД). Модель типизированной матрицы доступов. Основные положения модели. Теорема о существовании алгоритма проверки безопасности ациклических систем монотонных ТМД.
5. Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant. Модель распространения прав доступа Take-Grant. Теоремы о передаче прав в графе доступов, состоящем из субъектов, и произвольном графе доступов. Расширенная модель Take-Grant и ее применение для анализа информационных потоков в АС.
6. Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы. Модель Белла-Лападулы как основа построения систем мандатного разграничения доступа. Основные положения модели. Базовая теорема безопасности (BST). Политика low-watermark в модели Белла-ЛаПадулы.
Модуль 3. Модели безопасности информационных потоков и изолированной программной среды. Ролевая модель доступа.

7. Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений. Применение модели Биба для реализации мандатной политики целостности. Применение модели систем военных сообщений для систем приема, передачи и обработки почтовых сообщений, реализующих мандатную 8 политику безопасности. Шесть теоретических принципов политики контроля целостности. Соответствие правил модели Кларка-Вилсона принципам политики целостности.

8. Модели компьютерных систем с ролевым управлением. Понятие ролевого управления доступом. Базовая модель ролевого управления доступом. Понятие администрирования ролевого управления доступом. Администрирование иерархии ролей. Понятие мандатного ролевого управления доступом. Требования либерального мандатного управления доступом.

9. Модели безопасности информационных потоков и изолированной программной среды. Автоматная модель безопасности информационных потоков. Вероятностная модель безопасности информационных потоков. Информационное невлияние. Информационное невлияние с учетом фактора времени. Монитор безопасности объектов. Монитор безопасности субъектов. Теоремы о достаточных условиях гарантированного выполнения политики безопасности в компьютерных системах. Базовая теорема изолированной программной среды.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Операционные системы»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 3 зачетные единицы, 108 академических часа.

Форма промежуточной аттестации: зачет.

Цели и задачи освоения дисциплины

Основной целью дисциплины «Операционные системы» является дать целостное представление об архитектуре современных операционных систем (ОС).

Задачи дисциплины «Операционные системы»:

- познакомить с историей развития ОС;
- дать представление об основных функциях, принципах построения и видах ОС;
- дать представление о методах управления основными вычислительными ресурсами ЭВМ;
- дать представление об управлении устройствами ввода-вывода;
- познакомить с общими подходами к реализации файловых систем и организацией популярных файловых систем;
- познакомить с архитектурой современных ОС.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-7: способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ПК-2: способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований.

В результате изучения дисциплины студент должен:

знать:

- историю развития ОС;
- основные функции ОС, принципы построения ОС, основные архитектурные решения, применяемые при разработке ОС;
- основные подсистемы современных ОС и их назначение;
- принципы управления основными вычислительными ресурсами ЭВМ;
- принципы управления процессами и потоками;
- технологии управления памятью;
- принципы организации ввода-вывода;
- структуру современных файловых систем и технологии распределения дискового пространства;

- принципы организации взаимодействия прикладного ПО с ОС и аппаратным обеспечением;
- архитектуру современных ОС;

уметь:

- применять полученные знания при разработке программного обеспечения (организация взаимоисключающего доступа к критическим ресурсам, методы борьбы с тупиками и пр.);
- применять полученные знания при формировании комплекса мер по обеспечению информационной безопасности ОС;
- получать системную информацию о ресурсах ЭВМ;
- применять полученные знания при администрировании и защите ОС;
- использовать программные методы синхронизации процессов;
- использовать программные методы работы с памятью;
- применять полученные знания к различным предметным областям;
- работать с технической литературой и специализированными информационными ресурсами.

Краткое содержание дисциплины

Тема 1. Введение в ОС. Архитектура, функции, принципы построения, классификация ОС.
Тема 2. Управление процессами, алгоритмы планирования.
Тема 3. Синхронизация процессов. Тупики.
Тема 4. Управление памятью.
Тема 5. Организация ввода -вывода в ОС.
Тема 6. Файловая система. Общие положения.
Тема 7. Обзор современных файловых систем.
Тема 8. ОС семейства Windows NT. Общий обзор, архитектура.
Тема 9. Unix-like системы. Общий обзор, архитектура.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Организационное и правовое обеспечение информационной безопасности»
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»

Объем дисциплины (модуля): 5 зачетных единиц, 180 академических часов.

Форма промежуточной аттестации: экзамен (10 семестр).

Цели и задачи освоения дисциплины (модуля)

Целью преподавания дисциплины «Организационное и правовое обеспечение информационной безопасности» является раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, понятие и виды компьютерных преступлений, а также приобретение студентами знаний по организационному обеспечению защиты информации и формирование некоторых практических навыков работы.

Задачи дисциплины– дать основы:

- информационного законодательства Российской Федерации;
- правил лицензирования и сертификации в области защиты информации;
- международного законодательства в области защиты информации;
- знаний о компьютерных преступлениях;
- построения систем организационной защиты объектов информатизации

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-5: способностью использовать нормативные правовые акты в своей профессиональной деятельности

ОПК-9: способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации

ПК-6: способностью участвовать в разработке проектной и технической документации

ПК-14: способностью организовать работы по выполнению режима защиты информации, в том числе ограниченного доступа

ПК-16: разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем

В результате изучения дисциплины студент должен:

знать:

- нормативные правовые акты Российской Федерации в области обработки и защиты персональных данных, их содержание, предмет регулирования и сферу применения;

- основные понятия, термины и определения в области обработки и защиты персональных данных;
- основные угрозы безопасности информации;
- этапы создания системы защиты информации;
- виды защищаемой информации и информационных систем, требования по их защите;
- порядок проведения аттестации объекта информатизации;
- правила разработки технического задания на создание АС в защищенном исполнении;
- правила разработки технического проекта на создание системы защиты информации;
- необходимые для написания документов НПА и ГОСТы;
- порядок внедрения режима коммерческой тайны;
- порядок отнесения сведений к гостайне;
- грифы секретности и уровни допуска к гостайне;
- состав и принципы написания организационно-распорядительной документации по защите информации;
- способы использования и обозначения требований по защите информации в организационно-распорядительной документации;

уметь:

- применять нормативные правовые акты Российской Федерации в области обработки и защиты персональных данных для конкретных задач и ситуаций в области защиты информации;
- сформировать перечень требований по защите информационной системы;
- разрабатывать проекты документов Техническое задание и Технический проект на создание системы защиты информации;
- определять порядок и состав действий по внедрению коммерческой тайны;
- разрабатывать проекты организационно-распорядительной документации по защите персональных данных;

Краткое содержание дисциплины (модуля)

Тема 1. Законодательство РФ в сфере информационной безопасности
Тема 2. Практика правонарушений в области ИБ
Тема 3. Государственная система защиты информации РФ
Тема 4. Организация режима коммерческой тайны
Тема 5. Защита государственной тайны
Тема 6. Документация в области ИБ
Тема 7. Лицензируемая деятельность в области ИБ
Тема 8. Проектирование системы защиты информации
Тема 9. Аттестация объектов информатизации

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Основы информационной безопасности»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 3 зачетных единицы, 108 академических часа.

Форма промежуточной аттестации: зачет (6 семестр).

Цели и задачи освоения дисциплины (модуля)

Учебная дисциплина «Основы информационной безопасности» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной целью дисциплины «Основы информационной безопасности» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации; обучение основам информационной безопасности, принципам и методам защиты информации в информационных системах.

Задачи дисциплины «Основы информационной безопасности»:

- изучение основных методов и принципов обеспечения конфиденциальности, целостности и доступности информации в информационных системах;
- изучение типовых угроз безопасности информации при её обработке в информационных системах;
- изучение основных принципов обеспечения информационной безопасности;
- изучение основ построения модели угроз и политики безопасности;
- изучение основных моделей доступа.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

ОПК-3: способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации

ОПК-5: способностью использовать нормативные правовые акты в своей профессиональной деятельности

В результате изучения дисциплины студент должен:

знать:

- основные понятия информационной безопасности;
- важность и необходимость информационной безопасности на человека, организации и государства;

- уровни обеспечения информационной безопасности РФ;
- ответственность за преступления в информационной сфере в соответствии с законодательством РФ;
- основные регуляторы в области информационной безопасности;
- основные термины и определения в области теории информации, информационных технологий и защиты информации;
- основные угрозы информационной безопасности;
- основные методы обеспечения безопасности информационных систем;
- основные методы поиска информации из открытых источников;
- нормативные правовые акты Российской Федерации в области защиты информации, их содержание, предмет регулирования и сферу применения.

уметь:

- оценить возможные последствия противоправных действий в области информационных технологий;
- классифицировать информационные системы;
- классифицировать угрозы безопасности информации;
- применять нормативные правовые акты Российской Федерации в области защиты информации для конкретных задач и ситуаций.

Краткое содержание дисциплины (модуля)

Тема 1. Основные понятия теории информационной безопасности
Тема 2. Классификация угроз информационной безопасности
Тема 3. Основные механизмы обеспечения информационной безопасности
Тема 4. Теоретический подход к обеспечению информационной безопасности
Тема 5. Нормативно-правовой подход к обеспечению информационной безопасности
Тема 6. Практический (экспериментальный) подход к обеспечению информационной безопасности
Тема 7. Построение модели угроз
Тема 8. Определение и разработка политики безопасности
Тема 9.Аудит информационной безопасности

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Разработка и защита web-приложений»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 7 зачетных единиц.

Форма промежуточной аттестации: зачет, экзамен.

Цели и задачи освоения дисциплины (модуля)

Целью дисциплины «Разработка и защита web-приложений» является обучение студентов основам создания веб приложений, ознакомиться с современным серверным и сетевым оборудованием, изучить методики и способы защиты веб приложений и сетевого оборудования.

Задачи дисциплины «Разработка и защита web-приложений»:

- изучить устройство сети Интернет;
- изучить языки разметки документов;
- изучить протоколы http, https, ftp;
- изучить принцип работы веб сервера;
- принципы функционирования веб приложений;
- изучить средства разработки веб приложений;
- изучить наиболее распространённые веб серверы, их возможности и функционал;
- научиться создавать простейшие веб страниц;
- научиться использовать основные и дополнительные метатеги;
- изучить способы создания и настройки дополнительных инструментариев, позволяющие увеличивать посещаемость сайтов;
- изучить методы проверки и тестирования законченных сайтов;
- изучить подходы к проектированию веб сервера и локально-вычислительной сети с сетевым оборудованием;
- научиться организовывать способы защиты от различного рода сетевых атак на Web и DNS серверы, и сетевое оборудование;
- рассмотреть наиболее распространенные типы уязвимостей на сетевое оборудование;
- научиться настраивать веб сервер и его сетевые карты, роли DNS, IIS и другие для корректной работы сайта;
- научиться настраивать межсетевые экраны, коммутаторы, балансировку нагрузки;
- научиться организовывать серверные кластеры;
- научиться производить анализ защищенности веб приложения;
- научиться организовывать защиту веб приложений.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-8 – способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач.

В результате изучения дисциплины студент должен:

Знать:

- устройство сети Интернет;
- языки разметки документов;
- протоколы http, https, ftp;
- принцип работы веб сервера;
- принципы функционирования веб приложений;
- средства разработки веб приложений;
- наиболее распространённые веб серверы, их возможности и функционал;
- способы создания простейших веб страниц;
- основные и дополнительные метатеги;
- способы создания и настройки дополнительных инструментариев, позволяющие увеличивать посещаемость сайтов;
- методы проверки и тестирования законченных сайтов;
- подходы к проектированию веб сервера и локально-вычислительной сети с сетевым оборудованием;
- способы защиты от различного рода сетевых атак на Web и DNS серверы, и сетевое оборудование;
- наиболее распространенные типы уязвимостей.

Уметь:

- использовать средства разработки веб приложений;
- разрабатывать простые веб страницы на языке html;
- использовать основные и дополнительные метатеги;
- использовать дополнительный инструментарий, позволяющий увеличивать число посетителей и продвигать сайт в поисковых системах;
- настраивать веб сервер и его сетевые карты, роли DNS, IIS и другие для корректной работы сайта;
- настраивать межсетевые экраны, коммутаторы, балансировку нагрузки; организовывать серверные кластеры;
- производить анализ защищенности веб приложения;
- производить защиту веб приложения; производить устранение основных типов угроз.

Краткое содержание дисциплины (модуля)

5 семестр

Тема 1. Введение. Устройство сети Интернет. Обзор современных веб технологий.

Тема 2. DNS сервер и его роль в организации работы сайта.

Тема 3. DNS записи, маршрутизация и обзор современных DNS серверов.

и пересылки запросов DNS. Для этого: 1. Используя любую редакцию ОС MS Windows Server, выполнить настройки сетевого адаптера и присвоить ему статический IP-адрес. 2. Установить роль DNS. 3. Создать одну зону прямого просмотра (имя зоны назначаете самостоятельно). 4. Внести соответствующие записи необходимых типов в базу DNS. 5. Настроить зону обратного просмотра. 6. Организовать передачу зоны на другой доверенный сервер.

Тема 4. Языки разметки документов. Гипертекстовая разметка XML.

Тема 5. Средства разработки веб приложений. CMS – Системы управления контентом веб-сайтов.

Тема 6. Протокол HTTP, веб сервер и веб клиент, прокси сервер.

Тема 7. Создание простой web-страницы. Форматирование.

Тема 8. Каскадные таблицы стилей (CSS).

Тема 9. Метатеги основные и дополнительные.

Тема 10. Системы индексации сайтов. Файл robots.txt и sitemap.xml.

Тема 11. Веб-аналитика. Счетчики.

Тема 12. JavaScript для WEB.

6 семестр

Тема 13. Защищенное делегирование с DNSSEC.
Тема 14. Межсетевые экраны. Настройка межсетевого экрана модели DFL-860e.
Тема 15. Способы реализации процесса балансировки нагрузки.
Тема 16. Веб сервер и DNS сервер. Виртуализация серверов и ролей.
Тема 17. Почтовый сервер. Принцип работы, настройка и администрирование.
Тема 18. Способы защиты от спама.
Тема 19. Организация антивирусной защиты на серверах и шлюзах.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Разработка и защита мобильных приложений»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 7 зачетных единиц.

Форма промежуточной аттестации: зачет, экзамен.

Цели и задачи освоения дисциплины (модуля)

Разработка и защита мобильных приложений обеспечивает приобретение знаний и умений в соответствии с Федеральным государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цель дисциплины «Разработка и защита мобильных приложений» - является изложение теоретических и практических принципов разработки и защиты мобильных приложений с учетом современных тенденций.

Задачи курса - изучение:

- устройства платформы Android
- системного подхода к проектированию и созданию мобильных приложений
- архитектуры мобильного приложения, основных его компонентов
- основ разработки интерфейсов мобильных приложений
- основ разработки многооконных приложений
- основ работы с базами данных SQLite
- предотвращения угроз безопасности мобильных приложений

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-10: способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

ОПК-7: способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ОПК-8: способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач;

ПК-8: способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы;

В результате изучения дисциплины студент должен:

Знать:

1) этапы и тенденции развития программирования, способы применения ИТ при разработке мобильных приложений.
2) особенности применения сервисных программ и оболочек при разработке мобильных приложений.
3) содержание рынка программных продуктов и информационных услуг, тенденции, развитие и особенности рынка.

Уметь:

- выбрать оптимальный программный продукт и модели информационных технологий из нескольких возможных для решения прикладной задачи, и провести сравнительную оценку эффективности.
- выбрать программный продукт и технологии для решения задачи с учетом конкретной предметной области и провести анализ эффективности использования ПО для решения задач в предметной области.
- разрабатывать сервисные программы и сервисные оболочки при разработке мобильных приложений с учетом конкретной предметной области.

Краткое содержание дисциплины (модуля)

Дисциплина включает 3 темы:

Модуль 1. Общие сведения.

1. Введение в разработку мобильных приложений. Основные принципы разработки для ОС Android. Устройство платформы Android. Обзор сред программирования для Android. Возможности отладки на эмуляторах и реальных устройствах.
2. Виды приложений и их структура. Особенности видов мобильных приложений. Организация исполнения приложений в ОС Android и каким образом обеспечивается безопасная среда их функционирования.
3. Основы архитектуры приложения, основных его компонентов. Активности (Activities). Сервисы (Services). Контент-провайдеры (Content providers).

Модуль 2. Основы разработки мобильных приложений.

4. Основы разработки интерфейсов мобильных приложений. Графический дизайн и пользовательские интерфейсы. Визуальный информационный дизайн. Обзор интерфейса.
5. Основы разработки многооконных приложений. Многооконные приложения. Работа с диалоговыми окнами. Особенности разработки приложения, содержащего несколько активностей.
6. Использование возможностей смартфона в приложениях. Отличительные особенности смартфонов. Сенсорное (touch) управление. Взаимодействие с системами позиционирования

Модуль 3. Комплексные мобильные приложения.

7. Основы работы с базами данных SQLite. Основы SQL.Типы данных. Операторы. Выражения. Практическое использование SQLite в мобильных приложениях. Создание базы данных и таблиц. Получение системных данных. Работа с данными в SQLite.
8. Новое поколение инструментальных средств разработки мобильных приложений. Обзор возможностей Intel XDK. Эмулятор и запуск на устройстве.
9. Безопасность мобильных приложений. Введение в безопасность мобильных приложений. Статистические данные угроз безопасности мобильных приложений. Методы обнаружения уязвимостей в мобильных приложениях. Метод тестирования на проникновение. Генерация запросов по шаблону с типизированными параметрами. Метод статического анализа. Метод динамического анализа. Уязвимости, приводящие к выполнению кода. Переполнение буфера. Атака на функции форматирования строк. Внедрение операторов LDAP. Выполнение команд операционной системы. Внедрение операторов SQL. Внедрение SQL кода вслепую. Внедрение серверных расширений.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Сети и системы передачи информации»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 8 зачетных единиц.

Форма промежуточной аттестации: 3 семестр – зачет, 4 семестр – экзамен.

Цели и задачи освоения дисциплины (модуля)

Цель дисциплины «Сети и системы передачи информации» – изучение методов и средств построения и эксплуатации программно-аппаратных технологий, изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий передачи информации.

Задачи курса – изучение:

- принципов построения, функционирования и применения аппаратных средств современной вычислительной техники;
- основных теоретических концепций, положенных в основу построения современных компьютеров, вычислительных систем, сетей и телекоммуникаций.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8: способностью к самоорганизации и самообразованию;

ПК-10: способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации ;

ПК-5: способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

В результате изучения дисциплины студент должен:

Знать:

- способы аппаратной защиты беспроводной передачи информации;
- способы программной защиты беспроводной передачи информации;
- назначение и функции элементов аппаратной технологии защиты;
- организацию и структуру программной технологии защиты
- протоколы передачи информации;
- возможные угрозы при беспроводной передачи информации;
- организацию системной магистрали, способы подключения дополнительных устройств.

Уметь:

- формализовать поставленную задачу;
- настраивать беспроводные средства передачи информации;
- разбираться в устройствах рабочих станций и серверов;

- разбираться в телекоммуникационных устройствах передачи данных
- осуществлять обоснованный выбор стандартного периферийного оборудования;
- применять полученные знания к различным предметным областям.

Владеть:

- методами анализа основных электрических характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений, анализа сетевых протоколов;
- программными средствами построения моделей сетевого взаимодействия и сетевой топологии.

Краткое содержание дисциплины (модуля)

Дисциплина включает 18 тем:
Тема 1. Введение.
Тема 2. Коммуникации с помощью сетей.
Тема 3. Модель OSI. Уровень приложений и транспортный уровень.
Тема 4. Сетевой уровень модели OSI.
Тема 5. Адресация в сети – IPv4.
Тема 6. Канальный и физический уровни модели OSI.
Тема 7. Ethernet.
Тема 8. Планирование и монтаж сети.
Тема 9. Конфигурирование и тестирование сети.
Тема 10. Статическая маршрутизация.
Тема 11. Динамическая маршрутизация.
Тема 12. Дистанционно-векторные протоколы маршрутизации.
Тема 13. RIP, VLSM и CIDR.
Тема 14. RIPv2.
Тема 15. Таблицы маршрутизации.
Тема 16. EIGRP.
Тема 17. Протоколы маршрутизации по состоянию канала.
Тема 18. OSPF.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Системы управления базами данных»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 3 зачетные единицы.

Форма промежуточной аттестации: зачет.

Цели и задачи освоения дисциплины (модуля)

Цель дисциплины «Системы управления базами данных» - формирование у студентов совокупности профессиональных качеств, обеспечивающих решение проблем, связанных с проектированием и реализацией прикладных защищенных решений и баз данных под управлением современных систем управления базами данных (СУБД).

Задачи курса:

- обучить студентов принципам работы современных систем управления базами данных;
- привить студентам навыки проектирования и реализации баз данных;
- дать студентам представление о проектировании и эксплуатации реляционных баз данных.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8: способностью к самоорганизации и самообразованию

ПК-10: способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

В результате изучения дисциплины студент должен:

Знать:

- области применения систем управления базами данных;
- особенности управления данными в системах распределенной обработки;
- работы с системами управления базами данных на различных платформах;

Уметь:

- разрабатывать программы на высокоуровневых языках программирования
- применять навыки разработчика и администратора баз данных

Краткое содержание дисциплины (модуля)

Дисциплина включает 12 тем:

Тема 1. История развития, назначение и роль баз данных
Тема 2. Общие принципы построения БД. Модели данных
Тема 3. Основы построения реляционных БД
Тема 4. Физическая организация баз данных
Тема 5. Нормализация базы данных

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Теоретико-числовые методы в криптографии»
Специальность: 10.05.01 «Компьютерная безопасность» специализация
«Безопасность распределенных компьютерных систем» форма
обучения очная

Объем дисциплины (модуля): 3 зачетные единицы.

Форма промежуточной аттестации: зачет.

Цели и задачи освоения дисциплины (модуля)
Целью дисциплины «Теоретико-числовые методы в криптографии» является изложение базовых принципов построения и математического обоснования криптографических систем.

Задачи курса - изучение:
- Теоретико-числовых, алгебраических, аналитических и вероятностных подходов к построению и анализу криптосистем; - Математические основ криптографии;
- Математических методов, используемых в криптоанализе

Планируемые результаты освоения
В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-2 - способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов;

ПК-5 – способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

В результате изучения дисциплины студент должен:

Знать:
- теоретико-числовые основы двухключевой криптографии; основы дискретной алгебры и теории чисел; алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах;
- основные задачи и понятиях криптографии; основные виды асимметричных криптографических алгоритмов.

Уметь:

- проводить оценку сложности алгоритмов; выполнить постановку задач криптоанализа и указать подходы к их решению; использовать основные математические методы, применяемые в синтезе и анализе типовых криптографических алгоритмов;
- корректно применять симметричные и асимметричные криптографические алгоритмы; формализовать поставленную задачу.

Краткое содержание дисциплины (модуля) Дисциплина
включает 7 тем:
Тема 1. Введение в математические проблемы криптографии. Основы теории чисел.
Тема 2. Теория сравнений. Вычеты.
Тема 3. Сравнения первой степени. Системы сравнений первой степени
Тема 4. Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.
Тема 5. Порождающий элемент и дискретный логарифм. Криптосистемы на их основе.
Доказуемо простые числа.
Тема 6. Алгоритмы криптоанализа шифров с открытым ключом
Тема 7. Конечные группы и поля многочленов

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Техническая защита информации»
Специальность 10.05.03 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Трудоемкость дисциплины: 4 з.е., 144 часа

Форма промежуточной аттестации: экзамен

Цели и задачи освоения дисциплины:

Дисциплина «Техническая защита информации» является дисциплиной профессионального цикла ООП подготовки специалистов. Учитывая, что в ходе профессиональной деятельности специалисты этого направления будут иметь дело с информацией различного рода и различного уровня секретности, знание основных способов и средств съёма и защиты информации позволит им успешно решать профессиональные задачи. Дисциплина «Техническая защита информации» посвящена изучению основных каналов распространения информации и способов защиты информации в этих каналах от несанкционированного доступа.

Целью дисциплины «Техническая защита информации» является теоретическая и практическая подготовленность специалиста к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в защищаемых помещениях.

Задачами дисциплины являются:

ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;

ознакомление с техническими каналами утечки акустической (речевой) информации;

изучение способов и средств защиты информации, обрабатываемой техническими средствами;

изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации; изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;

обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

Планируемые результаты освоения дисциплины:

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-1: способностью анализировать физические явления и процессы для решения профессиональных задач;

ПК-12 - способностью проводить инструментальный мониторинг защищенности компьютерных систем;

ПК-19 - способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации;

ПК-9 - способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы.

В результате изучения дисциплины «Технические средства и методы защиты информации» студенты должны:

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;

Краткое содержание дисциплины

1. Введение. Характеристика государственной системы противодействия технической разведке
2. Обнаружение и локализация источников радиоизлучений
3. Нормативные документы по противодействию технической разведке
4. Цифровые диктофоны
5. Демаскирующие признаки объектов наблюдения и сигналов
6. Генераторы радиошума и блокираторы источников радиосигналов
7. Средства и методы технической разведки
8. Обнаружение и локализация закладных устройств с помощью нелинейного локатора
9. Способы и средства перехвата сигналов. Способы и средства наблюдения
10. Многофункциональные поисковые приборы, ST-031 «Пиранья»
11. Технические каналы утечки информации
12. Универсальный анализатор проводных линий «УЛАН-2»
13. Оптические и радиоэлектронные каналы утечки информации
14. Акустоэлектрические преобразователи
15. Акустические и виброакустические каналы утечки информации
16. Многофункциональные поисковые приборы, ST-032
17. Средства обнаружения технических каналов утечки информации
18. Детектор электромагнитного поля ST 007
19. Мероприятия по выявлению средств технической разведки
20. Принципы дозиметрической разведки. Дозиметрия ионизирующих излучений
21. Методы и средства защиты информации от утечки по техническим каналам
22. Обнаружение и локализация акустических закладных устройств, программный коррелятор «OSCOR»
23. Скрытие речевой информации в каналах связи
24. Измерение ПЭМИ монитора и оценка величины зоны R2
25. Обнаружение и локализация закладных устройств
26. Изучение устройства и работы лазерного микрофона
27. Концепция и методы инженернотехнической защиты информации
28. Генераторы акустического и виброакустического шума
29. Виды контроля и расчёта эффективности защиты информации
30. Дополнительная лабораторная работа
31. Виды контроля и расчёта эффективности защиты информации

32. Дополнительная лабораторная работа

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
ТЕХНОЛОГИИ И МЕТОДЫ ПРОГРАММИРОВАНИЯ
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 7 зачетных единиц.
Форма промежуточной аттестации: зачет(5 семестр), экзамен(6 семестр).
Цели и задачи освоения дисциплины (модуля)

Учебная дисциплина «Технологии и методы программирования» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Технологии и методы программирования» является изложение основополагающих принципов разработки программного обеспечения в различных средах с использованием различных информационных технологий при решении разнообразных прикладных задач.

Задачи дисциплины «Технологии и методы программирования»

- дать представление о компьютерных технологиях и методах программирования;
- научить использовать компьютерные технологии и методы программирования для решения разнообразных прикладных задач.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
ОПК-8 - способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач;
ОПК-10 - способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах.

В результате изучения дисциплины студент должен:
знать:

- основные языки и системы программирования, среды разработки и компьютерные технологии;
- способы построения, анализа и реализации алгоритмов.

уметь:

- применять основные языки и системы программирования, среды разработки и компьютерные технологии в профессиональной деятельности;
- проводить построение, анализ и реализацию алгоритмов в современных программных комплексах.

Краткое содержание дисциплины (модуля)
1. Введение в дисциплину
2. Разработка с использованием скриптовых языков программирования.
3. Разработка Win32 приложений и библиотек

4. Разработка консольных приложений
5. Разработка оконных приложений
6. Параллельное программирование
7. Разработка и использование COM объектов
8. Разработка и использование ActiveX объектов
9. Разработка сетевых приложений
10. Разработка сервисных приложений
11. Разработка .NET-приложений
12. Разработка внешних хранимых процедур для серверов баз данных
13. VBA приложения
14. Web приложения

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Электроника и схемотехника»
Специальность: 10.05.01 Компьютерная безопасность
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины: 4 з.е. (144 часа)

Форма промежуточной аттестации: экзамен.

Цели и задачи освоения дисциплины

Целью дисциплины «Электроника и схемотехника» является изучение основ электроники, элементов теории сигналов и схемотехники преобразовательных, усилительных и генераторных элементов в информационных сетях, системах автоматизации.

Задачами дисциплины являются:

– ознакомление студентов с основами преобразования электрических сигналов в линейных и нелинейных аналоговых и цифровых цепях;

– ознакомление с элементной базой электротехнических и электронных цепей;

– ознакомление с основными принципами преобразования электромагнитной энергии в устройствах усиления, выпрямления и генерации;

– ознакомление со схемотехникой аналоговых и цифровых устройств;

– получение практических навыков исследования радиоэлектронных устройств.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

– способностью к самоорганизации и самообразованию (ОК-8);

– способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-5);

– способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации (ПК-11);

– способностью проводить инструментальный мониторинг защищенности компьютерных систем (ПК-12);

– способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации (ПК-19).

В результате изучения дисциплины студент должен:

знать:

– содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности;

- основные принципы работы и проектирования электронных систем; особенности применения аналоговых и цифровых радиоэлектронных устройств;
- основные параметры и принципы работы базовых аналоговых и цифровых функциональных элементов электроники;
- основные физические понятия и принципы функционирования базовых электронных полупроводниковых компонентов в аналоговых и цифровых системах;
- терминологию и символику, используемую в электронике, методы составления и чтения основных видов электрических схем;
- особенности применения аналоговых и цифровых радиоэлектронных устройств.

уметь:

- самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
- рассчитывать простые аналоговые и цифровые радиоэлектронные устройства;
- оценивать степень достоверности результатов, полученных с помощью экспериментальных и теоретических методов исследований;
- проводить базовые теоретические и экспериментальные исследования электронного оборудования и систем;
- проводить контрольные проверки работоспособности применяемых средств защиты информации.

Краткое содержание дисциплины

Тема 1. Полупроводниковые приборы.
Тема 2. Биполярные транзисторы.
Тема 3. Усилители электрических сигналов.
Тема 4. Дифференциальный каскад.
Тема 5. Генераторы электрических колебаний.
Тема 6. Элементы цифровой электроники.
Тема 7. Сигналы и их классификация.
Тема 8. Прохождение гармонического сигнала через нелинейную цепь.

Темы лабораторных занятий:

Лабораторная работа №1. Исследование диодов.
Лабораторная работа №2. Исследование биполярного транзистора.
Лабораторная работа №3. Исследование инвертирующего и неинвертирующего усилителя на операционном усилителе.
Лабораторная работа №4. Исследование логических элементов цифровых интегральных микросхем.
Лабораторная работа №5. Исследование JK-триггера и счетчика.
Лабораторная работа №6. Исследование параметрического стабилизатора напряжения.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Языки программирования»
10.05.01 Компьютерная безопасность
Специализация: безопасность распределенных компьютерных систем
Форма обучения очная

Объем дисциплины (модуля): 13 *з.е.*

Форма промежуточной аттестации: зачет, экзамен

Цели и задачи освоения дисциплины (модуля):
Цель дисциплины: освоение базовых конструкция языка программирования высокого уровня; изучение стандартных типов данных языка программирования высокого уровня; овладение умением конструирования пользовательских типов данных; получение знаний о приёмах алгоритмизации, о формальной постановке задачи, об основных этапах реализации программ на компьютере; формирование готовности использовать приобретенные знания в профессиональной деятельности.

Задачи дисциплины:
- получение знаний, составляющих основу научных представлений об информации, информационных процессах, системах, технологиях и моделях; приобретении практических навыков работы с различными видами информации с помощью компьютера и других средств информационных и коммуникационных технологий;
- обучение студентов основным подходам к проектированию, разработке и использованию программ;
- дать обучающимся знание технологий разработки программного обеспечения с использованием универсальных языков программирования.

Планируемые результаты освоения
Освоение дисциплины способствует формированию у обучающихся следующих компетенций:
ОПК-8: способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач.
ОПК-10: способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах.

В результате освоения дисциплины обучающийся должен:
Знает: основные направления развития технологий программирования, виды основных структур данных, их особенности, основные методы решения типовых численных задач, методы решения профессиональных, исследовательских и прикладных задач: основные концептуальные положения процедурного программирования, основные методы реализации соответствующих алгоритмов с помощью ЭВМ; алгоритмы и технологии программирования для разработки приложений, осуществляющих решение типовых задач.

Умеет: формализовать вычислительную задачу и выбрать необходимый типовой алгоритм для ее решения; выявить типовые, а также нестандартные задачи, разработать метод решения поставленной задачи с использованием типовых алгоритмов; разрабатывать специализированные программы для решения задач, тестировать и отлаживать программы в интегрированной среде разработки; опираясь на знания теоретических основ программирования, оптимизировать исходный код.

Краткое содержание дисциплины (модуля)

Освоение дисциплины предполагает последовательное освоение следующих тем:

1. Введение в C#. Система типов языка C#. Выражения и операторы. Управление действиями с данными. Массивы.
2. Основные принципы и этапы ООП. Классы и объекты. Элементы класса. Поля и методы. Свойства объектов.
3. Наследование в C#.
4. Виртуальные и динамические методы. Полиморфизм.
5. Абстрактные классы. Интерфейсы. Исключения. Делегаты и события
6. Основы визуального программирования на языке C#.
7. Использование стандартных компонент пользовательского интерфейса
8. Разработка многооконных приложений. Стандартные окна диалога. Файловые типы данных.
9. Организация механизма Drag&Drop.
10. Построение графических изображений.
11. Организация многопоточных приложений.
12. Основы языка Python.
13. Организация работы с файлами в Python.
14. Функции в Python.
15. Основы ООП в Python.
16. Технологии доступа к данным.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Безопасность распределенных компьютерных систем»
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единицы.

Форма промежуточной аттестации: экзамен.

Цели и задачи освоения дисциплины (модуля)

Целью дисциплины «Безопасность распределенных компьютерных систем» является обучение студентов основам проектирования защищенных автоматизированных систем, ознакомление с оборудованием и организации защиты датчиков, автоматизированных узлов и диспетчерских.

Задачи дисциплины «Безопасность распределенных компьютерных систем»:

- изучить современные технологические процессы и их технологию;
- основную нормативно-техническую документацию;
- изучить виды оборудования и принципы работы;
- изучить всевозможные угрозы, влияющие на работу оборудования и технологического процесса в целом;
- научиться строить модели нарушителя для предложенной технологической линейки или технологии;
- научиться настраивать оборудование;
- научиться строить принципиальные и подробные электрические схемы, в том числе с использованием эмуляторов и имитационных тренажеров;

научиться разрабатывать мнемосхемы и скада системы для предложенного технологического процесса.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ПК-8 – способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы.

В результате изучения дисциплины студент должен:

Знать:

- нормативно-техническую документацию;
- принцип работы оборудования автоматизированных систем;
- программное обеспечение для моделирования автоматизированных систем;
- способы защиты оборудования и узлов автоматизированных систем;
- способы проведения анализа, а также подбора оборудования и средств защиты для предложенного технологического процесса;
- методики чтения технологических схем;
- системы автоматизированного проектирования схем, сетей и узлов.

Уметь:

- применять нормативно-техническую документацию;
- проводить экспериментально-исследовательские работы с оборудованием и сетями автоматизированных систем;
- настраивать защиту оборудования и проводить мониторинг специальными средствами;
- применять навыки для проведения анализа, а также подбора оборудования и средств защиты для предложенного технологического процесса;
- Анализировать предложенные структурные и принципиальные технологические схемы и сети автоматизированных систем и узлов;
- Разрабатывать технологические и принципиальные схемы, а также проводить соответствующие расчеты при подборе оборудования и автоматизированных узлов.

Краткое содержание дисциплины (модуля)

Тема 1. Введение. Обзор современных автоматизированных систем и устройств.
Тема 2. Система теплоснабжения зданий различного назначения. Учет и регулировка теплоносителя.
Тема 3. Тепловые счетчики, их устройство и режимы работы.
Тема 4. Интерфейсы RS-232, RS-422 и RS-485.
Тема 5. Система погодного регулирования. Система управления газовыми и твердотопливными котлами.
Тема 6. ТРМ32 контроллер для отопления и ГВС. СУНА-121 контроллер для групп насосов. Угрозы и аварийные ситуации.
Тема 7. Установки и устройства для поддержания микроклимата в помещениях/зданиях различного назначения. Модели угроз.
Тема 8. Системы охранно-пожарной сигнализации и пожаротушения. Организация диспетчерских пультов.
Тема 9. Системы видеонаблюдения. Проектирование сетей охранного телевидения. Виды оборудования. Защита данных.
Тема 10. Системы диспетчеризации. Их обустройство. Принципиальные схемы.
Тема 11. Среда проектирования Codesys. Алгоритмы работы контроллера ПЛК-150.
Тема 12. Принципы конфигурирования оборудования автоматизации.
Тема 13. Моделирование сетей и узлов систем автоматизации в различных средах. Имитационные модели.
Тема 14. Разработка Скада-систем.

Аннотация к рабочей программе дисциплины
Современные системы виртуализации
Специальность: 10.05.01. Компьютерная безопасность
Специализация: Безопасность распределенных компьютерных систем
форма обучения очная

Объем дисциплины (модуля): 4 з.е.

Форма промежуточной аттестации: зачет (8 семестр).

Цели и задачи освоения дисциплины (модуля)

В ходе изучения дисциплины обучающиеся приобретают теоретические и практические навыки реагирования на инциденты, их расследования, поиска цифровых следов в компьютерных системах, фиксации этих следов в качестве доказательств по гражданским и уголовным делам, анализа собранных материалов с целью выявления источника атаки и восстановления работоспособности системы, а также документирования противоправных действий злоумышленников.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-7. способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения.

ПК-17. способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение.

В результате изучения дисциплины студент должен:

Знать:

- технологии для DevOps;
- технологии виртуализации;
- гипервизоры 1,2 уровней;
- методы обеспечения отказоустойчивости;
- методы резервного копирования;
- принципы функционирования Docker;
- kubernetes и оркестрацию контейнеров;
- технологию централизованного управления логами;
- компоненты ИТ-инфрасруктуры;
- особенности операционных систем (ОС) Linux;
- основные принципы и команды CLI;
- основы администрирования в ОС Linux;

Уметь:

- устанавливать и настраивать основные инфраструктурные компоненты для проектирования и разработки информационных систем;
- выполнять базовые функции администрирования ОС Linux;
- работать с CLI и системными утилитами;
- конфигурировать локальные сети;
- устанавливать и настраивать инструменты разработчика и необходимые библиотеки;
- управлять репозиторием проекта (локальным и удалённым);
- настраивать гипервизоры 1,2 уровней;

- настраивать и проводить мониторинг инфраструктуры;
- настраивать централизованное управление логами;
- работать с Graylog, ELK, RabbitMQ, Zabbix.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Безопасность сетей электронно-вычислительных машин»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единицы.

Форма промежуточной аттестации: экзамен.

Цели и задачи освоения дисциплины (модуля)

Цель дисциплины "Безопасность сетей электронно-вычислительных машин" - является изложение основополагающих принципов разработки сетевого программного обеспечения в различных средах с использованием различных информационных технологий при решении разнообразных прикладных задач.

Задачи курса - изучение:

- основных принципов разработки сетевых протоколов;
- основных принципов анализа сетевых протоколов;
- принципов разработки сетевых программ и выбора технологии и протокола передачи данных.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8 - способность к самоорганизации и самообразованию;

ПК-5 - способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-10 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-18 - способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

В результате изучения дисциплины студент должен:

Знать:

- принципы функционирования протоколов FTP, HTTP, SMTP и POP3, стандартные
- команды протоколов;
- назначение, преимущества и недостатки протоколов FTP, HTTP, SMTP и POP3;
- протоколы FTP, HTTP, SMTP и POP3;
- Basic, Digest, NTLM и авторизацию с помощью форм.

Уметь:

- производить основные действия с протоколами FTP, HTTP, SMTP или POP3 программно;
- производить проверку безопасности реализации протоколов FTP, HTTP, SMTP и POP3;
- разрабатывать положения, инструкции и других организационно- распорядительные документы необходимые для обеспечения ИБ при использовании протоколов FTP, HTTP, SMTP и POP3;
- настраивать Basic, Digest, NTLM и авторизацию с помощью форм.

Краткое содержание дисциплины (модуля)

Дисциплина включет 9 тем:

Тема 1. Основные понятия.

Тема 2. Протокол HTTP.

Тема 3. Протокол FTP.

Тема 4. Протокол POP3.

Тема 5. Протокол SMTP.

Тема 6. Уязвимости сетевых протоколов.

Тема 7. Обзор современных сетевых протоколов.

Тема 8. Разработка сетевых приложений на базе протокола TCP.

Тема 9. Анонимные и именованные каналы связи.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Безопасность систем баз данных»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единицы.

Форма промежуточной аттестации: экзамен.

Цели и задачи освоения дисциплины (модуля)

Цель дисциплины «Безопасность систем баз данных» - формирование у студентов совокупности профессиональных качеств, обеспечивающих решение проблем, связанных с использованием и проектированием баз данных под управлением современных систем управления базами данных (СУБД), а также связанных с обеспечением безопасности информации в автоматизированных информационных системах (АИС), основу которых составляют базы данных (БД) навыкам работы со встроенными в системы управления базами данных (СУБД) средствами защиты.

Задачи курса - изучение:

• обучить студентов принципам работы современных систем управления базами данных;
• привить студентам навыки проектирования и реализации баз данных;
• приобретение системного подхода к проблеме защиты информации в СУБД;
• изучение моделей и механизмов защиты в СУБД;
• приобретение практических навыков организации защиты БД.
• обучить студентов проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований;
• обучить студентов формализовать поставленную задачу по обеспечению защиты БД;
• обучить студентов применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
• привить студентам навыки разработки нормативных и организационнораспорядительных документов, регламентирующих работу по защите информации в СУБД

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8: способностью к самоорганизации и самообразованию;

ПК-10: способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-18: способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

В результате изучения дисциплины студент должен:

В результате изучения дисциплины студент должен:

Знать:

- современные критерии и стандарты для анализа безопасности информационных систем на базе СУБД;
- основные средства и способы обеспечения информационной безопасности, предоставляемые системами управления базами данных;
- сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
- средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;

Уметь:

- анализировать и оценивать угрозы информационной безопасности объекта;
- применять отечественные и зарубежные стандарты для проектирования, разработки и оценивания защищенности компьютерной системы;
- 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.

Краткое содержание дисциплины (модуля)

Дисциплина включет 9 тем:

Тема 1. Безопасность БД, угрозы, защита
Тема 2. Критерии защищенности БД
Тема 3. Модели безопасности в СУБД
Тема 4. Средства идентификации и Аутентификации
Тема 5. Средства управления доступом
Тема 6. Целостность БД и способы ее обеспечения
Тема 7. Классификация угроз конфиденциальности СУБД
Тема 8. Аудит и подотчетность
Тема 9. Транзакции и блокировки

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Высшая математика»
Специальность 10.05.01 Компьютерная безопасность
Специализация: Безопасность распределенных компьютерных систем
форма обучения - очная

Трудоемкость дисциплины: 16 зачетных единиц, 576 академических часов.

Форма промежуточной аттестации: 2 семестр – экзамен, 3 семестр – экзамен, 4 семестр – экзамен, 5 семестр – экзамен.

Цели и задачи освоения дисциплины

Целями преподавания дисциплины являются:

- формирование и развитие навыков математического мышления, навыков использования математических методов и основ математического моделирования, математической культуры у обучающихся;
- обеспечение высокого уровня фундаментальной математической подготовки студентов, необходимого для дальнейшего обучения и успешного усвоения специальных дисциплин;
- приобретение навыков самостоятельного изучения отдельных тем дисциплины и решения типовых задач;
- усвоение полученных знаний студентами, а также формирование у них мотивации к самообразованию за счет активизации их познавательной деятельности.

Задачи изучения дисциплины:

- формирование у студентов базовых знаний об основных математических объектах и структурах,
- освоение методов работы с указанными объектами;
- изучение алгоритмов решения типовых задач;
- обзор возможностей применения изученных моделей и методов к решению различных задач.

Планируемые результаты освоения

Код и наименование компетенции (из ФГОС ВО)	Код и наименование части компетенции (при наличии паспорта компетенций)	Компонент (знаниевый/функциональный)

Способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов. (ОПК-2)	ОПК-2	Знает основные понятия, теоремы и методы алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, использующихся при изучении общетеоретических и специальных дисциплин учебного цикла; Уметет использовать знания фундаментальных основ, подходы и методы математики при решении прикладных задач; пользоваться источниками для самостоятельного изучения специальной литературы;

Краткое содержание дисциплины

Основные понятия. Алгебра матриц. Операции над матрицами. Определители и из свойства. Линейные пространства. Ранг матриц. Системы линейных уравнений. Ранг матриц. Аксиоматика линейных пространств. Линейные операторы. Образ и ядро линейного оператора. Координаты векторов. Евклидовы и унитарные пространства. Связь матриц линейного оператора в различных базисах. Процесс ортогонализации. Ранг и дефект. Метод ортогонализации. Линейные операторы в евклидовых и унитарных пространствах. Собственные векторы и значения. Унитарные операторы. Эрмитовы операторы. Ортогональные операторы. Квадратичные формы. Приведение квадратичной формы к главным осям. Элементы теории множеств. Множества. Последовательности. Предел последовательности. Функции. Предел функции. Непрерывные функции. Производная функции. Дифференцирование функций. Исследование функций. Построение графиков функций. Функции многих переменных. Экстремумы функций многих переменных. Исследование функций многих переменных. Интегрирование. Неопределенный интеграл. Определенный интеграл. Дифференциальные уравнения. Дифференциальные уравнения 2 порядка. Числовые ряды. Сходимость рядов. Числовые ряды. Функциональные ряды. Степенные ряды. Основные алгебраические структуры. Группы. Кольца. Поля. Кольцо вычетов. Сравнения. Сравнения с одним неизвестным. Сравнения второй степени. Кольцо целых чисел. Поле комплексных чисел. Тригонометрическая форма комплексного числа. Кольцо многочленов. Деление многочленов. Корни многочленов. Многочлены над произвольным полем. Кольцо вычетов. Важнейшие функции теории чисел. Разложение на множители. Трансцендентные числа. Функции Мёбиуса и Эйлера. Основные комбинаторные конфигурации. Элементы комбинаторики. Методы перечисления. Производящие функции. Распределение простых чисел в арифметических прогрессиях. Основные понятия теории графов. Графы. Остовы и деревья. Деревья. Сеть. Поток. Разрез. Побуквенное кодирование. Оптимальные коды. Логика высказываний. Формулы алгебры логики. Булевы функции. Совершенные формы. Предполные классы булевых функций. Исчисление высказываний. Секвенции. Логика предикатов. Предварено нормальная форма. Фильтры, теорема компактности. Исчисление предикатов. Вычислимые функции. Частично рекурсивные функции. Машина Тьюринга. Функции, вычислимые на машине Тьюринга.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Дополнительные главы информационной безопасности»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 5 зачетных единиц.

Форма промежуточной аттестации: зачет.

Цели и задачи освоения дисциплины (модуля)
Целью дисциплины «Дополнительные главы информационной безопасности» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации; систематизация знаний, а также совершенствование умений и навыков, необходимых для построения эффективной системы защиты информации.
Задачи дисциплины «Дополнительные главы информационной безопасности»: описание различных подходов к организации процесса проверки подлинности сущностей информационной безопасности; теоретическая и практическая проработка моделей разграничения прав доступа; изучение методик проведения аудита информационной безопасности и теста на проникновение; освоение методов учета и анализа действий пользователей в информационной системе; обучение навыкам решения задач информационной безопасности с помощью возможностей машинного обучения.

Планируемые результаты освоения
В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8 - способностью к самоорганизации и самообразованию
ПК-1 - способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности;
ПК-2 - способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований;
ПК-8 - способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы;
ПСК-3.4 - способностью организовывать защиту информации в распределенных компьютерных системах.

В результате изучения дисциплины студент должен:

Знать:
- различные подходы к организации процесса проверки подлинности сущностей информационной безопасности;
- теоретическую базу моделей разграничения прав доступа;
- методики проведения аудита информационной безопасности и теста на проникновение

- методы учета и анализа действий пользователей в информационной системе;
- методы решения задач информационной безопасности с помощью возможностей машинного обучения.

Уметь:

- применять различные подходы к организации процесса проверки подлинности сущностей информационной безопасности;
- применять модели разграничения прав доступа на практике;
- применять методики проведения аудита информационной безопасности и теста на проникновение;
- применять методы учета и анализа действий пользователей в информационной системе;
- применять методы решения задач информационной безопасности с помощью возможностей машинного обучения.

Краткое содержание дисциплины (модуля)

Лекция 1. Введение в информационную безопасность. Основные понятия и определения.
Определение информационной безопасности. Определение конфиденциальности, целостности и доступности информации. Определение угрозы, уязвимости и эксплойта. Словари уязвимостей. Основные способы обеспечения информационной безопасности.

Лекция 2. Классификация угроз информационной безопасности.
Классификация угроз информационной безопасности информационных систем по ряду базовых признаков: по природе возникновения, по степени преднамеренности появления, по непосредственному источнику угроз, по положению источника угроз, по степени зависимости от активности информационной системы, по степени воздействия на информационную систему и т.д.

Лекция 3. Аутентификация: проверка подлинности пользователей.
Определение аутентификации как процесса проверки подлинности субъекта. Аутентификация вида «клиент-система», сетевая аутентификация. Биометрические методы аутентификации. Аутентификация с помощью электронно-цифровой подписи. Аутентификация с помощью пары «логин/пароль». Протокол Radius, Kerberos.

Лекция 4. Авторизация: разграничение прав доступа.
Авторизация как основной механизм разграничения прав доступа. Основные модели разграничения прав доступа: дискреционная модель, мандатная модель, ролевая модель доступа, модель изолированной программной среды, модель безопасности информационных потоков.

Лекция 5. Обзор отечественных стандартов ИБ и их сравнение с зарубежными стандартами.
Объекты правового регулирования при создании и эксплуатации системы защиты информации. Использование существующих нормативных актов для создания системы информационной безопасности. Основные положения руководящих правовых документов. История создания TCSEC («Оранжевая книга»). Основные положения Руководящих документов ФСТЭК в области защиты информации. Стандарт ГОСТ Р ИСО/МЭК 15408 (на основе текста стандарта ISO 15408), обзор стандартов группы ИСО/МЭК 27000 (на основе серии стандартов ISO/IEC 27000).
Лекция 6. Структура системы защиты информации.
Комплексный подход к обеспечению информационной безопасности. Понятие политики безопасности, модели политики безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Мандатная политика целостности. Политика информационной безопасности как основа организационных мероприятий. Контроль и

моделирование как основные формы организационных действий при проверке действенности системы информационной безопасности. Разграничение прав доступа как основополагающее требование организационных мероприятий и их практическая реализация на объекте защиты.

Лекция 7. Основные элементы системы защиты информации.
Описание основных элементов системы защиты информации (IDS/IPS, SIEM, DLP, брандмауэр и т.д.).

Лекция 8. Аудит информационной безопасности.
Аудит системы информационной безопасности. Определение уровня защищённости информационной системы. Аудит системы информационной безопасности на объекте как основание для подготовки организационных и правовых мероприятий. Его критерии, формы и методы. Алгоритм проведения аудита информационной безопасности.

Лекция 9. Анализ и оценка рисков информационной безопасности.
Количественная и качественная оценки рисков. Методики анализа и оценки рисков информационной безопасности.

Планы практических занятий

Практическое занятие 1. Объекты и субъекты информационной безопасности.
Определение объектов и субъектов информационной безопасности в информационной системе.

Практическое занятие 2. Угрозы информационной безопасности.
Проведение классификации угроз информационной безопасности в информационной системе.

Практическое занятие 3. Аутентификация.
Реализация аутентификации пользователей с использованием пары «логин/пароль».

Практическое занятие 4. Авторизация.
Сравнительный анализ и реализация дискреционной, мандатной и ролевой моделей доступа.

Практическое занятие 5. Отечественные стандарты ИБ и их сравнение с зарубежными стандартами.
Обеспечение безопасности информационной системы в соответствии со стандартом ГОСТ Р ИСО/МЭК 15408 и стандартами группы ИСО/МЭК 27000.

Практическое занятие 6. Построение системы защиты информации.
Разработка и обоснование политики безопасности для информационной системы. Реализация принципа глубокой эшелонированности обороны в соответствии с комплексным подходом к обеспечению информационной безопасности.

Практическое занятие 7. Элементы системы защиты информации.
Настройка брандмауэра и IDS.

Практическое занятие 8. Аудит информационной безопасности.
Подготовка пакета документов в рамках проведения аудита информационной безопасности.

Практическое занятие 9. Анализ текущего уровня защищенности информационной системы.
Анализ защищенности системы по методу CRAMM.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Защита государственных информационных систем и персональных данных»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

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

Форма промежуточной аттестации: экзамен (10 семестр).

Цели и задачи освоения дисциплины (модуля)

Учебная дисциплина «Безопасность персональных данных» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Программа дисциплины «Безопасность персональных данных» ориентирована на достижение следующих целей:

- получения знаний о принципах обработки персональных данных в РФ;
- освоение методов и способов построения системы защиты персональных данных.

Для достижения поставленной цели предусмотрены следующие задачи:

- изучить основные нормативно-правовые акты в области защиты персональных данных и области их применения;
- изучить алгоритмы классификации информационных систем персональных данных;
- научить обучающихся строить модели нарушителя и угроз безопасности информации;
- сформировать у обучающегося навыки правильного обоснованного выбора мер по защите информации и аргументированно исключать не подходящие
- научить обучающихся разрабатывать проект системы защиты информации, обрабатываемой в информационных системах персональных данных.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8 - способность к самоорганизации и самообразованию;

ПК-6 - способность участвовать в разработке проектной и технической документации;

ПК-7 - способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем;

ПК-16 - способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем;

ПСК-3.5 - способность участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем.

В результате изучения дисциплины студент должен:

знать:

- нормативные правовые акты Российской Федерации в области обработки и защиты персональных данных, их содержание, предмет регулирования и сферу применения;
- основные понятия, термины и определения в области обработки и защиты персональных данных;
- отечественные нормативно-правовые акты, методические документы и стандарты в области защиты информации и защиты персональных данных;

- существующие базы знаний и информационные системы нормативных правовых актов РФ;
- правовые основания обработки персональных данных;
- необходимые параметры и характеристики информационной системы персональных данных, необходимые для определения требуемого уровня защищенности персональных данных;
- основные угрозы безопасности персональных данных;
- состав и принципы написания организационно-распорядительной документации по защите информации;
- способы использования и обозначения требований по защите информации в организационно-распорядительной документации;
- правила разработки технического задания на создание АС в защищенном исполнении;
- правила разработки технического проекта на создание системы защиты персональных данных;
- необходимые для написания документов НПА и ГОСТы;
- нормативные и методические документы ФСТЭК России и ФСБ России по моделированию нарушителя и угроз безопасности информации;
- методику определения угроз безопасности персональных данных в соответствии с требованиями законодательства РФ;
- отечественные нормативно-правовые акты и методические документы в области защиты информации и защиты персональных данных, описывающие требования и меры по защите персональных данных;
- методику формирования набора организационных и технических мер по защите информации;
- основные классы и характеристики средств защиты информации;
- правила подбора средств защиты информации для обеспечения необходимого уровня защищенности персональных данных.

уметь:

- применять нормативные правовые акты Российской Федерации в области обработки и защиты персональных данных для конкретных задач и ситуаций в области защиты информации;
- использовать средства поиска информации в сети Интернет;
- использовать специальные информационные системы, базы знаний и электронные библиотеки для поиска и работы с нормативными правовыми документами;
- осуществлять подбор и анализ нормативных правовых документов и информации необходимых для решения конкретных задач по обработке и защите персональных данных;
- определять тип обрабатываемых персональных данных и правовые основания их обработки и хранения;
- определять уровень защищенности персональных данных при их обработке в информационных системах персональных данных;
- построить модель нарушителя и модель угроз информационной безопасности персональных данных;
- разрабатывать проекты организационно-распорядительной документации по защите персональных данных;
- разрабатывать проекты документов Техническое задание и Технический проект на создание системы защиты персональных данных;

- построить модель нарушителя и модель угроз информационной безопасности персональных данных;
- формировать набор требований по обеспечению безопасности персональных данных;
- формировать набор и определять состав организационных и технических мер по защите персональных данных;
- осуществлять подбор средств защиты информации;
- определять состав контрольных и периодических мероприятий по поддержке реализованной в системе защите персональных данных политики безопасности.

Краткое содержание дисциплины (модуля)

Тема 1. Законодательство по защите персональных данных
Тема 2. Информационные системы персональных данных
Тема 3. Обследование информационных систем
Тема 4. Модель нарушителя безопасности персональных данных
Тема 5. Модель угроз безопасности персональных данных
Тема 6. Определение состава требований и мер по защите персональных данных
Тема 7. Мероприятия по защите персональных данных

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Защита корпоративных систем»
Направление подготовки:
10.05.01 «Компьютерная безопасность (специалитет)»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единиц.

Форма промежуточной аттестации: экзамен

Цели и задачи освоения дисциплины (модуля)

- Цель дисциплины «Защита корпоративных систем» является изучение программных способов и методов защиты современных сетевых сервисов и протоколов маршрутизации, а также - изучение основных подходов к эксплуатации технологий защиты при передаче информации в сети предприятия.

Задачи курса:

- Анализ принципов функционирования и защиты современных протоколов маршрутизации в сети предприятия;
- Организация безопасных базовых сервисов в сети предприятия средствами современного телекоммуникационного оборудования;
- Изучение функциональных возможностей современных технологий защиты передачи информации в сети предприятия.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ПСК-3.2 - способность анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем;

ПСК-3.3 - способность использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности;

ПСК-3.5 - способность участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем.

В результате изучения дисциплины студент должен:

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.

Краткое содержание дисциплины (модуля)

Дисциплина включает 9 тем:

Тема 1. Защита программ и данных в компьютерной сети

Тема 2. Маршрутизация в сети предприятия

Тема 3. Статические маршруты для IPv4 / IPv6

Тема 4 Защита протокола RIP.

Тема 5 Защита протокола EIGRP.

Тема 6. Защита протокола OSPF.

Тема 7. Подключение сети предприятия к сети Интернет с использованием протокола BGP.

Тема 8. Защита основных сервисов сети предприятия

Тема 9. Защита передаваемых по сети данных.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Научно-проектный (исследовательский) семинар»
10.05.01 «Компьютерная безопасность (специалитет)»
специализация «Безопасность распределенных компьютерных систем»

Объем дисциплины (модуля): 9 зачетных единиц, 324 академических часов.

Форма промежуточной аттестации: Зачет (7,8 семестр).

Цели и задачи освоения дисциплины (модуля)

Основной целью дисциплины является развитие навыков студента для проведения самостоятельной научно-исследовательской работы.

Задачи дисциплины – дать основы:

- развить навыки поиска, изучения, обобщения и систематизации научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности;
- научить правилам оформления списка литературных источников;
- навыками проведения научно-исследовательской работы и применения методов научных исследований в профессиональной деятельности;
- развить навыки разработки научно-технических отчетов, обзоров, публикаций по результатам выполненных работ;
- дать опыт публичной защиты собственного научного труда.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями: ОК-8, ОПК-4, ПК-1.

В результате изучения дисциплины студент должен:

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.

Краткое содержание дисциплины (модуля)

1. Актуальные проблемы и научно-исследовательские задачи в области ИБ
2. Презентация и обсуждение тем проектов
3. Поиск и систематизация научной информации. Работа с литературой.
4. Представление и обсуждение литературного обзора по теме проекта
5. Подготовка научно-технического отчета

6. Презентация и обсуждение плана реализации проекта
7. Правила презентации научного исследования
8. Презентация и обсуждение промежуточных результатов реализации проекта
9. Презентация и обсуждение результатов реализации проекта

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Организация электронно-вычислительных машин и вычислительных систем»

специальность 10.05.01 «Компьютерная безопасность»

специализация «Безопасность распределенных компьютерных систем» очной формы обучения

Трудоемкость дисциплины: 8 з.е., 288 час.

Форма промежуточной аттестации: экзамен (3 семестр), экзамен (4 семестр)

Цели и задачи освоения дисциплины

Цель дисциплины — обучить студентов общим принципам построения и эксплуатации аппаратных средств вычислительной техники и методов ее функционирования в локальных и глобальных вычислительных сетях.

Задачи дисциплины:

- обучение систематизированным представлениям о принципах построения и архитектурных особенностях различных классов электронно-вычислительных машин (ЭВМ);
- изложение основных концепций, представления, хранения и обработки данных в ЭВМ;
- изучение принципов работы микропроцессорных систем.

Планируемые результаты освоения

В результате освоения образовательной программы, выпускник должен обладать следующими профессиональными компетенциями:

- способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения (ОПК-7)

В результате изучения дисциплины студент должен

знать:

- основные этапы создания и развития ЭВМ;
- существующие виды архитектур ЭВМ, назначение и функции ее элементов;
- 2-х, 8-ми, 10-ти, 16-ти -ричную арифметики;
- основы теории кодирования данных;
- основы теории построения логических схем;
- организацию и структуру центрального процессора, памяти, системы прерывания, системы ввода вывода;

— организацию системной магистрали, способы подключения дополнительных устройств;
— физические основы и принципы действия периферийных устройств, интерфейсы периферийных устройств;
— основы языка низкого уровня.

уметь:

— формализовать поставленную задачу;
— осуществлять программную реализацию алгоритма;
— разбираться в устройстве рабочих станций, ноутбуков, серверов;
— применять полученные знания к различным предметным областям.

владеть навыками:

— изучения компонентов компьютера с помощью инструкций на языке ассемблера;
— оценки конфигурации вычислительной системы с точки зрения требуемых функциональных возможностей;
— оценки программно-аппаратной конфигурации вычислительной системы с точки зрения компьютерной безопасности.

Краткое содержание дисциплины

— История вычислительной техники, поколения и классификация ВТ
— Архитектура и структура ЭВМ
— Основные элементы и периферийные узлы ЭВМ
— Представление данных в ЭВМ. Кодирование
— Логические основы функционирования ЭВМ
— Основы построения цифровых логических цепей, принципы организации памяти
— Организация микропроцессорной техники
— Основы языка ассемблера
— Основы файловых систем
— Основы операционных и файловых систем семейства Windows
— Понятие и принципы функционирования BIOS/UEFI
— Сменные носители информации — флэш- память, оптические носители
— Звуковые карты
— Современные микропроцессорные технологии
— Материнская плата персонального компьютера. Шины расширения. Интерфейсы
— Видеоподсистема
— Устройства ввода/вывода. Печатающие и сканирующие устройства
— Мобильные платформы
— Оперативная память ЭВМ
— Электропитание ЭВМ
— Дисковая память ЭВМ. RAID массивы. Восстановление данных
— Серверные и многопроцессорные комплексы (суперкомпьютеры)
— Микроконтроллеры. Однокристальные системы

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Программно-аппаратные средства обеспечения информационной безопасности»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 8 зачетных единиц, 288 академических часа.

Форма промежуточной аттестации: зачет (9 семестр), экзамен (10 семестр).

Цели и задачи освоения дисциплины (модуля)

Учебная дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» является теоретическая и практическая подготовка работе с современными отечественными средствами защиты информации и внедрение их в систему защиты информации.

Для достижения поставленной цели предусмотрены следующие задачи:

- изучить типы и виды средств защиты информации;
- дать представление о существующих отечественных и зарубежных средствах защиты информации;
- научить устанавливать, настраивать и администрировать средства защиты информации;
- научить делать обоснованный выбор средства защиты информации при проектировании системы защиты информации.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8: способность к самоорганизации и самообразованию;

ПК-5: способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-18: способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-20: способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций.

В результате изучения дисциплины студент должен:

знать:

- дополнительные источники получения информации по администрированию средств защиты;

- основные угрозы безопасности информации;
- требования к обеспечению ИБ различными техническими мерами;
- принципы работы и основной функционал средств защиты информации;
- порядок сертификации средств защиты информации в РФ;
- варианты и формы сертификации средств защиты информации в РФ;
- виды сертифицируемых средств защиты информации и предъявляемые им требования по безопасности;
- основные типы и виды средств защиты информации, принципы их действия;
- основные модули и функциональные возможности средств защиты информации;
- требования к среде функционирования средства защиты информации;
- принципы функционирования модулей средств защиты информации;
- способы влияния средств защиты информации на программное окружение;
- варианты зависимости работоспособности средств защиты информации от программного окружения;
- основные виды и типы средств защиты информации;
- основной функционал различных видов средств защиты информации;
- требования по обеспечению ИБ для различных ИС;
- правила выбора средств защиты информации в различных ИС;
- отечественные средства защиты информации;

уметь:

- находить необходимую дополнительную информацию по средству защиты на сайте компании-производителя;
- сопоставлять реализуемый средствами защиты информации функционал с предъявляемыми требованиями по ИБ;
- определять нейтрализуемые средствами защиты информации угрозы;
- формулировать требования к конфигурированию средств защиты информации;
- выбрать необходимый способ сертификации средства защиты информации;
- составить план сертификации средства безопасности;
- определить состав требований, предъявляемых к сертифицируемому средству защиты информации и к компании-заявителю;
- настраивать среду функционирования перед установкой средств защиты информации;
- устанавливать, настраивать и удалять средства защиты информации;
- применять различные конфигурации средств защиты информации в зависимости от параметров информационной системы;
- проводить проверку работоспособности средств защиты информации
- анализировать журнал событий средств защиты информации;
- осуществлять сохранение настроек средства защиты информации и их восстановление;
- поиск причин нарушения работоспособности средства защиты информации;
- определить виды средств защиты информации в зависимости от предъявляемых требований;
- обоснованно подобрать необходимые модели и марки средств защиты информации;

Краткое содержание дисциплины (модуля)

Тема 1.Классификация и виды средств защиты информации.
Тема 2. Система сертификации средства защиты информации в РФ.
Тема 3. Средства доверенной загрузки.
Тема 4. Средства защиты от несанкционированного доступа.
Тема 5. Средства криптографической защиты информации.
Тема 6. Средства антивирусной защиты.

Тема 7. Средства анализа и контроля защищенности.
Тема 8. Выбор технических мер при проектировании системы защиты информации.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«**Системы видеонаблюдения**»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация: «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единицы.

Форма промежуточной аттестации: зачет.

Цели и задачи освоения дисциплины (модуля)

Целью дисциплины «Системы видеонаблюдения» является обучение студентов основам проектирования систем видеонаблюдения, ознакомиться с современным оборудованием, изучить методики расчета и подбора оборудования, изучить технологические схемы, используемые в сблокировке с охранно-пожарными и другими системами.

Задачи дисциплины «Системы видеонаблюдения»:

- изучить основную нормативно-техническую документацию;
- изучить основные принципы и подходы при организации технической защиты информации;
- изучить методики расчета и подбора оборудования видеонаблюдения;
- изучить архитектуру сетей видеонаблюдения;
- изучить некоторое сервисное программное обеспечение.
- изучить принципы и подходы к проектированию систем видеонаблюдения.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8 – способностью к самоорганизации и самообразованию.

ПК-14 – способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа.

В результате изучения дисциплины студент должен:

Знать:

- нормативно-техническую документацию;
- принцип работы оборудования видеонаблюдения;
- основные подходы к проектированию систем видеонаблюдения;
- способы организации физической и информационной защиты основного и вспомогательного оборудования.

Уметь:

- ориентироваться в нормативно-технической документации;
- разрабатывать и применять технические решения для объектов любой сложности;
- настраивать основное и вспомогательное оборудование;
- проектировать схемы на планах здания, разрабатывать структурные электрические схемы.

Краткое содержание дисциплины (модуля)

Тема 1. Введение. Назначение систем видеонаблюдения и их роль. Действующая нормативная документация. Федеральные законы.

Тема 2. Знакомство со средой автоматизированного проектирования AutoCad.

Тема 3. Знакомство и изучение реальных проектов и их технических решений.

Тема 4. Классификация систем видеонаблюдения. Общие требования, предъявляемые к системам видеонаблюдения.

Тема 5. Виды видеокамер и их устройство. Интерфейсы. Способы настройки и управления. Правила подбора. Датчики, сблокированные с камерами.

Тема 6. Виды объективов для видеокамер. Методика расчета и подбор.

Тема 7. Инфракрасные прожекторы, их расчет и подбор.

Тема 8. Кожухи и корпуса видеокамер камер. Обеспечение микроклимата. Методика расчета и подбор.

Тема 9. Виды видеорегистраторов. Правила подбора. Настройка.

Тема 10. Делитель экрана. Мультиплексор. Платы видеозахвата.

Тема 11. Сетевое оборудование для систем видеонаблюдения. Правила подбора. Расчет пропускной способности каналов.

Тема 12. Источники резервированного питания. Методика подбора. Расчет общей нагрузки. Привязка оборудования к индивидуальному или к центральному источнику питания.

Тема 13. Оборудование АРМ. Пульты управления. Программные средства регистрации видеосигнала.

Тема 14. Типовые схемы видеонаблюдения. Простейшие схемы с одним видеорегистратором. Сложные схемы. Схемы, комбинированные с охранно-пожарной сигнализацией, системой СКУД и климатическим оборудованием.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Управление информационной безопасностью»
Специальность: 10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Объем дисциплины (модуля): 4 зачетные единицы.

Форма промежуточной аттестации: зачет.

Цели и задачи освоения дисциплины (модуля)

Целью дисциплины «Управление информационной безопасностью» - изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта (СУИБ).

Задачи курса - изучение:

- Формирование требований к системе управления ИБ конкретного объекта.
- Проектирование системы управления ИБ конкретного объекта.
- Эффективное управление ИБ конкретного объекта.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8 - способность к самоорганизации и самообразованию;

ПК-7 - способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем;

ПК-13 - способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности;

ПК-15 - способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы.

В результате изучения дисциплины студент должен:

Знать:

- историю информационных технологий;
- основные направления повышения надежности вычислительных систем, комплексов и сетей, а также методы и средства обеспечения безопасности и сохранности информации в них;
- основные принципы построения информационной безопасности;
- основные стандарты, регламентирующие управление ИБ;
- способы защиты информации в различных операционных системах; основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ.

Уметь:

- понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны;
- анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ;
- использовать 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;
- выделять основные методы организации информационной безопасности в условиях конкретной задачи;
- определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
- анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ.

Краткое содержание дисциплины (модуля) Модуль 1.

Основы управления ИБ.

1. Введение. Базовые вопросы управления ИБ. Процессный подход. Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием.

Стандартизация в области построения систем управления. История развития. Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов.

2. Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ. Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.). Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ.

3. Рискология ИБ. Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.

Модуль 2. Основные процессы СУИБ.

4. Основные процессы СУИБ. Обязательная документация СУИБ. Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы

улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик

эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».

5. Эксплуатация и независимый аудит СУИБ. Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации. Модуль 3.Процессы.

6. Внедрение разработанных процессов. Документ «Положение о применимости». Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБ, и способы их решения. Контроль над внедрением процессов. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.

7. Процесс «Управление инцидентами ИБ. Процесс «Обеспечение непрерывности ведения бизнеса». Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ. Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.

8. Обеспечение соответствия требованиям законодательства РФ. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.). Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

Аннотация к рабочей программе дисциплины
Современные системы виртуализации
Специальность: 10.05.01. Компьютерная безопасность
Специализация: Безопасность распределенных компьютерных систем
форма обучения очная

Объем дисциплины (модуля): 5 з.е.

Форма промежуточной аттестации: зачет (10 семестр).

Цели и задачи освоения дисциплины (модуля)

В ходе изучения дисциплины обучающиеся приобретают теоретические и практические навыки реагирования на инциденты, их расследования, поиска цифровых следов в компьютерных системах, фиксации этих следов в качестве доказательств по гражданским и уголовным делам, анализа собранных материалов с целью выявления источника атаки и восстановления работоспособности системы, а также документирования противоправных действий злоумышленников.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8. способностью к самоорганизации и самообразованию.

ПК-17. способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение.

В результате изучения дисциплины студент должен:

Знать:

- технологии для DevOps;
- технологии виртуализации;
- гипервизоры 1,2 уровней;
- методы обеспечения отказоустойчивости;
- методы резервного копирования;
- принципы функционирования Docker;
- kubernetes и оркестрацию контейнеров;
- технологию централизованного управления логами;
- компоненты ИТ-инфрасруктуры;
- особенности операционных систем (ОС) Linux;
- основные принципы и команды CLI;
- основы администрирования в ОС Linux;

Уметь:

- устанавливать и настраивать основные инфраструктурные компоненты для проектирования и разработки информационных систем;
- выполнять базовые функции администрирования ОС Linux;
- работать с CLI и системными утилитами;
- конфигурировать локальные сети;
- устанавливать и настраивать инструменты разработчика и необходимые библиотеки;
- управлять репозиторием проекта (локальным и удалённым);
- настраивать гипервизоры 1,2 уровней;
- настраивать и проводить мониторинг инфраструктуры;
- настраивать централизованное управление логами;

- работать с Graylog, ELK, RabbitMQ, Zabbix.

Аннотация к рабочей программе дисциплины
Компьютерная форензика и расследование инцидентов
Специальность: 10.05.01. Компьютерная безопасность
Специализация: Безопасность распределенных компьютерных систем
форма обучения очная

Объем дисциплины (модуля): 5 з.е.

Форма промежуточной аттестации: зачет (10 семестр).

Цели и задачи освоения дисциплины (модуля)

В ходе изучения дисциплины обучающиеся приобретают теоретические и практические навыки реагирования на инциденты, их расследования, поиска цифровых следов в компьютерных системах, фиксации этих следов в качестве доказательств по гражданским и уголовным делам, анализа собранных материалов с целью выявления источника атаки и восстановления работоспособности системы, а также документирования противоправных действий злоумышленников.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-8. способность к самоорганизации и самообразованию.

ПК-20. способность участвовать в разработке подсистемы информационной безопасности компьютерной системы.

В результате изучения дисциплины студент должен:

Знать:

- о компьютерной криминалистике и правовом обеспечении расследования инцидентов информационной безопасности;
- об анализе лог-файлов;
- об алгоритме расследования инцидентов информационной безопасности;
- о производстве компьютерно-технической экспертизы;
- об основных программных и аппаратных средствах поиска уликовых данных;
- о вскрытии защищенных данных, хранящихся в специализированных «контейнерах», запароленных архивах и т.п.

Уметь:

- искать утраченную или сокрытую информацию на компьютере и мобильных устройствах;
- документально оформлять процесс расследования инцидентов ИБ;
- документально оформлять процесс проведения компьютерно-технической экспертизы;

Владеть:

- навыками расследование инцидентов информационной безопасности;
- навыками производства компьютерно-технической экспертизы;
- навыками работы со специализированным программным и аппаратным обеспечением по проведению компьютерно-технической экспертизы.