НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

«УТВЕРЖДАЮ»

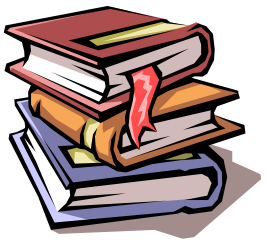
Декан ФРТиС

_____У.И. Медеуов

«____»_____2017 г.

КАТАЛОГ ЭЛЕКТИВНЫХ ДИСЦИПЛИН НА 2017 ГОД ПОСТУПЛЕНИЯ

Специальность 5В100200 «СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»



АЛМАТЫ 2017 г.

5В100200 – СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЭЛЕКТИВНЫЕ ДИСЦИПЛИНЫ
(по выбору)

№ п/п	Цикл дисциплин	Цифровой код дисциплин	Наименование дисциплины	Семестр	Кол-во кредитов
1	ООД	1106	Экологическая устойчивость и безопасность жизнедеятельности	1	3
		1106	Экологическая и техногенная безопасность		
2	ООД	1107	Политико-правовые и социально-духовные основы общества	1	4
		1107	Социальные институты современного общества: политика, право, религия		
3	БД	1209	Алгоритмизация и языки программирования	2	3
		1209	Основы программирования		
4	БД	1211	Основы информационной безопасности	2	2
		1211	Технологии информационной безопасности		
5	БД	1210	Операционная система Linux	2	2
		1210	Операционная система Unix		

ЭКОЛОГИЧЕСКАЯ УСТОЙЧИВОСТЬ И БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Постреквизиты: Охрана и защита труда.

Цель изучения: вооружить будущих специалистов теоретическими и практическими знаниями, необходимыми для: создания оптимальных условий труда; рационального размещения оборудования, устройства цехов энерго предприятий сельского хозяйства в соответствий с санитарно-гигиеническими и противопожарными требованиями; творческого решения вопросов, связанных с разработкой новой техники и технологий, исключающих производственный травматизм и профессиональную заболеваемость.

Краткое содержание (основные разделы): необходимость использования системного подхода при изучении вопросов обеспечения безопасности и охраны труда, выработать умение использовать нормативные и правовые акты, содержащие нормы безопасности и охраны труда, а также осуществлять контроль за их соблюдением; дать представление о взаимосвязи функциональных и психофизиологических возможностях человека и его совместимости с производственной средой; познакомить с мерами по

предотвращению и снижению рисков на рабочих местах и в технологических процессах.

Результаты изучения:

знать – решение различных вопросов в области охраны труда при проектировании и эксплуатации энергетических объектов;

уметь – создавать оптимальные условия труда, исключить производственный травматизм;

иметь навыки – организации, управления промышленной безопасностью, действующий на основании соответствующих законодательных и нормативных актов системы социально-экономических, организационных, технических, гигиенических и лечебно-профилактических мероприятий и средств, обеспечивающих безопасность сохранения здоровья и работоспособность человека в процессе жизнедеятельности;

компетенции – знать основы правовой системы и законодательство Казахстана при решение основных вопросов в области охраны труда при проектировании и эксплуатации энергетических объектов.

Кафедра – «Безопасность жизнедеятельности и защита окружающей среды».

ЭКОЛОГИЧЕСКАЯ И ТЕХНОГЕННАЯ БЕЗОПАСНОСТЬ

Постреквизиты: Охрана труда (Охрана и защита труда).

Цель изучения: теоретические и практические знания, необходимые для: создания оптимальных условий труда; рационального размещения оборудования, устройства цехов энергетических предприятий сельского хозяйства в соответствии с требованиями санитарно-гигиенической и противопожарной службой; творческого решения вопросов в разработке новых технологий, исключающих производственный травматизм и профессиональную заболеваемость.

Краткое содержание (основные разделы): использование системного подхода при изучении вопросов обеспечения экологической и техногенной безопасности, дать представление о системе мер, обеспечивающих с заданной вероятностью допустимое негативное воздействие факторов экологической опасности на окружающую среду и самого человека.

Результаты изучения:

знать – решение вопросов в области охраны труда при проектировании и эксплуатации различных объектов;

уметь – организовать рабочее место с соблюдением всех норм и правил, создавать оптимальные условия труда, исключить производственный травматизм;

иметь навыки – организации промышленной безопасностью, действующей на основании соответствующих законодательных и нормативных актов системы социально-экономических, организационных, технических и гигиенических мероприятий и средств, обеспечивающих безопасность здоровья человека в процессе жизнедеятельности;

компетенции – знать основные нормы экологической и техногенной безопасности в территориальных условиях Казахстана при решение основных вопросов в области охраны труда и эксплуатации различных объектов.
Кафедра – «Безопасность жизнедеятельности и защита окружающей среды».

ПОЛИТИКО-ПРАВОВЫЕ И СОЦИАЛЬНО-ДУХОВНЫЕ ОСНОВЫ ОБЩЕСТВА

Постреквизиты: Казахстанская модель социально-экономического развития.
Цель изучения – формирование у студентов системы знаний о политико-правовых и социально-духовных основах функционировании и развития общества.
Краткое содержание (основные разделы): основные этапы становления и развития политико-правовой мысли; социально-духовные основы общества; соотношение политических интересов личности и общества; проблемы формирования гражданского общества в Казахстане.
Результаты изучения:
знать - основы и закономерности развития политико-правовой и социально-нравственной жизни современного общества, различные научные подходы к актуальным проблемам современного человека и общества и особенностях их решения;
уметь - систематизировать знания о политике, праве, религии и их роли в жизни общества, вырабатывать свою гражданскую позицию и нести социальную ответственность перед обществом;
иметь навыки - анализа и оценки основ современного общества, коммуникации с помощью этих знаний в регулировании отношений в обществе, приобретения новых знаний, умений, в том числе в области, отличной от профессиональной;
компетенции – знать социально-этические ценности, основанные на общественном мнении, традициях, обычаях, политико-правовых нормах и ориентироваться на них в своей профессиональной деятельности.
Кафедра – «Социальные дисциплины».

СОЦИАЛЬНЫЕ ИНСТИТУТЫ СОВРЕМЕННОГО ОБЩЕСТВА: ПОЛИТИКА, ПРАВО, РЕЛИГИЯ

Постреквизиты: Теоретическая экономика и экономическая практика (Казахстанская модель социально-экономического развития).
Цель изучения - формирование у студентов основных научных знаний о социальных институтах современного общества, выработать у них научный подход к оценке тех или иных общественных событий и явлений, вооружить знаниями, необходимыми для творческого решения своих профессиональных проблем, формирования демократической культуры.
Краткое содержание (основные разделы): формирование социальных институтов; признаки, элементы и типология социальных институтов; предназначения, функции и дисфункции социальных институтов; политические институты; право, как социальный институт; религия как

социальный институт; современные социальные институты; социально-политическое развитие и модернизация современного казахстанского общества.

Результаты изучения:

знать - закономерности становления и развития социальных институтов, основные функции и дисфункции социальных институтов, роль социальных институтов для современного казахстанского общества;

уметь - самостоятельно анализировать, критически мыслить, формировать свой собственный подход в познании и оценке фактов, событий и явлений в общественной жизни;

иметь навыки - оценки достоверности информации, сопоставляя различные источники, анализа и оценки состояния и тенденций развития современного общества;

компетенции – знать тенденции социального развития общества.

Кафедра – «Социальные дисциплины».

АЛГОРИТМИЗАЦИЯ И ЯЗЫКИ ПРОГРАММИРОВАНИЯ

Постреквизиты: «Программирование на языках высокого уровня», «Прикладное программирование».

Цель изучения: изучение основных этапов решения задач на компьютерах, основ алгоритмизации, способов записи алгоритмов, алгоритмических языков высокого уровня, структуры программ, стиля программирования, типов данных, динамических структур данных, основных операторов языков высокого уровня, модульных программ, методов разработки программ, методов проектирования ПО, способов конструирования, отладки и верификации программ.

Краткое содержание дисциплины: ставит целью ознакомить студентов с принципами и методологией построения алгоритмов программных систем, сформировать у обучающегося навыки логического мышления и общую техническую культуру будущего специалиста.

Результаты изучения:

Знать:

- основные алгоритмические языки и их области применения;
- методы и свойства алгоритмов, принципы построения алгоритмов;
- структуры алгоритмов и программ, методы отладки и тестирования программ;
- основы алгоритмизации задач, типы данных, основные операторы языков высокого уровня;

модульные программы, элементы структурного программирования, стиль программирования.

Уметь:

- разрабатывать алгоритмы для решения различных задач;
- писать программы на алгоритмических языках на высоком профессиональном уровне, грамотно используя средства языка;
- отлаживать и тестировать программы, используя инструменты и справочную

службу программной среды;
- использовать стандартные библиотеки и встроенные возможности алгоритмических языков;
- использовать возможности вычислительных систем при разработки программ;
- применять методы и средства разработки алгоритмов и программ, приемы структурного программирования, способы записи алгоритма на языке высокого уровня, способы отладки и тестирования;
- составлять качественную программную документацию.

Иметь навыки:
- постановки задачи, разработки алгоритмов и программ;
- использования алгоритмических языков для решения задач;
- программирования в современных операционных средах;
- использования стандартных библиотек и модулей;
- использование технологии программирования для обработки информации.

Кафедра – Радиотехники и информационной безопасности.

ОСНОВЫ ПРОГРАММИРОВАНИЯ

Постреквизиты: «Программирование на языках высокого уровня», «Прикладное программирование».

Цель изучения: изучение основных этапов решения задач на компьютерах, основ алгоритмизации, способов записи алгоритмов, алгоритмических языков высокого уровня, структуры программ, стиля программирования, типов данных, динамических структур данных, основных операторов языков высокого уровня, модульных программ, методов разработки программ, методов проектирования ПО, способов конструирования, отладки и верификации программ.

Краткое содержание дисциплины: ставит целью ознакомить студентов с принципами и методологией построения алгоритмов программных систем, сформировать у обучающегося навыки логического мышления и общую техническую культуру будущего специалиста.

Результаты изучения:

Знать:
- основные алгоритмические языки и их области применения;
- методы и свойства алгоритмов, принципы построения алгоритмов;
- структуры алгоритмов и программ, методы отладки и тестирования программ;
- основы алгоритмизации задач, типы данных, основные операторы языков высокого уровня;

модульные программы, элементы структурного программирования, стиль программирования.

Уметь:
- разрабатывать алгоритмы для решения различных задач;
- писать программы на алгоритмических языках на высоком профессиональном уровне, грамотно используя средства языка;

- отлаживать и тестировать программы, используя инструменты и справочную службу программной среды;
- использовать стандартные библиотеки и встроенные возможности алгоритмических языков;
- использовать возможности вычислительных систем при разработки программ;
- применять методы и средства разработки алгоритмов и программ, приемы структурного программирования, способы записи алгоритма на языке высокого уровня, способы отладки и тестирования;
- составлять качественную программную документацию.

Иметь навыки:
- постановки задачи, разработки алгоритмов и программ;
- использования алгоритмических языков для решения задач;
- программирования в современных операционных средах;
- использования стандартных библиотек и модулей;

использование технологии программирования для обработки информации.

Кафедра – Радиотехники и информационной безопасности.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Математика».

Постреквизиты: «Криптографические методы и средства защиты», «Безопасность интернет технологий», «Правовое и информационное обеспечение информационной безопасности».

Цель изучения: изучение студентами вопросов хранения, восстановления секретной информации. Представлении информации в виде математических моделей, методах анализа информации, основах криптологии, криптографии, криптоанализа, стойкости шифров, кодировании, моделях систем шифрования.

Краткое содержание дисциплины: Типы угроз и объекты защиты. Источники потери информации и их предотвращение. Средства и способы защиты информации. Вредоносные программы и методы защиты от них. Антивирусные программы. Стандартные нормативы, регулирующие обеспечение защиты и безопасности информации. Перспективные технологии и системы организации обеспечения защиты и безопасности информации.

Результаты изучения:

Знать: определение и основные характеристики систем защиты информации; определение и основные характеристики систем обеспечения безопасности информации; основные методы и средства анализа информационных атак; основные методы и средства построения защищенных информационных систем; основные практические направления построения систем защиты и безопасности информации.

Уметь: оценивать типы угроз и объекты защиты информации; анализировать причины образования технических каналов утечки информации; использовать программные средства защиты информации; проводить физические

эксперименты, работы с измерительными приборами, расчет и обработку полученных данных.
Иметь навыки: использовать современные методы защиты и безопасности для решения поставленных задач.
Кафедра – Радиотехники и информационной безопасности.

ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Математика».
Постреквизиты: «Криптографические методы и средства защиты», «Безопасность интернет технологий», «Правовое и информационное обеспечение информационной безопасности».
Цель изучения: ознакомить студентов с вопросами хранения, поиска, преобразования, восстановления секретной информации. Дать знания о представлении информации в виде математических моделей, методах анализа информации, основах криптологии, криптографии, криптоанализа, стойкости шифров, кодировании, моделях систем шифрования.
Краткое содержание дисциплины: Основы защиты информации, элементы защиты, способы защиты от несанкционированного доступа к ней, средства и системы сбора и защиты информации.
Результаты изучения:
Знать: существующие угрозы безопасности информации, основные принципы защиты информации в компьютерных системах, причины, виды, каналы утечки и искажения информации, стандарты по оценке защищенных систем, основы криптографии, криптологии и криптоанализа, модели систем шифрования.
Уметь: Пользуясь литературой и справочниками, определять необходимые характеристики защищаемой информационной системы, составлять программу шифрования информации, определять каналы утечки и искажения информации.
Иметь навыки: о современных и перспективных направлениях развития защиты информации, о принципах криптографии, криптологии и криптоанализе, об существующих угрозах безопасности информации, о причинах, видах, каналов утечки и искажения информации, о достижениях современной теории защиты информации, владеть современными методами анализа защищенности информационных систем, о методе построения защищенной информационной системы.
Кафедра – Радиотехники и информационной безопасности.

ОПЕРАЦИОННАЯ СИСТЕМА LINUX

Постреквизиты: «Администрирование доменных систем».
Цель изучения: обучение методологическим основам принципов построения и функционирования средств реализации системного программного обеспечения вычислительных машин, систем и сетей.

Краткое содержание дисциплины: получение знаний, умений и навыков будущим специалистом, обеспечивающих обработку информации различных видов, решению функциональных и вычислительных задач на компьютере.
Результаты изучения:
Знать:
- технологию, методы и средства производства программного продукта;
- принципы построения современных ОС и системного программного обеспечения;
- технологии организации и построения вычислительных и операционных систем;
- классификацию операционных систем и устройств компьютера;
- общие принципы анализа и управления компонентами систем;
- принципы ввода-вывода информации на различные устройства.
Уметь:
- организовывать диалог с ЭВМ на базе командных языков программных оболочек;
- использовать системные программные средства, операционные системы и оболочки, обслуживающие сервисные программы;
- составлять программы для управления функционированием ЭВМ, систем и сетей;
Иметь навыки: работы с данными всех уровней организации файловой системы.
Кафедра – Радиотехники и информационной безопасности.

ОПЕРАЦИОННАЯ СИСТЕМА UNUX
Постреквизиты: «Администрирование доменных систем».
Цель изучения: обучение методологическим основам принципов построения и функционирования средств реализации системного программного обеспечения вычислительных машин, систем и сетей.
Краткое содержание дисциплины: получение знаний, умений и навыков будущим специалистом, обеспечивающих обработку информации различных видов, решению функциональных и вычислительных задач на компьютере.
Результаты изучения:
Знать:
- технологию, методы и средства производства программного продукта;
- принципы построения современных ОС и системного программного обеспечения;
- технологии организации и построения вычислительных и операционных систем;
- классификацию операционных систем и устройств компьютера;
- общие принципы анализа и управления компонентами систем;
- принципы ввода-вывода информации на различные устройства.
Уметь:
- организовывать диалог с ЭВМ на базе командных языков программных оболочек;

- использовать системные программные средства, операционные системы и оболочки, обслуживающие сервисные программы;
- составлять программы для управления функционированием ЭВМ, систем и сетей;

Иметь навыки: работы с данными всех уровней организации файловой системы.

Кафедра – Радиотехники и информационной безопасности.

№ п/п	Цикл дисциплин	Цифровой код дисциплин	Наименование дисциплины	Семестр	Кол-во кредитов
1	БД	2212	Технологии и методы программирования	3	3
		2212	Методологические основы программирования		
2	БД	2213	Архитектура компьютерных систем и сетей	3	3
		2213	Интерфейсы компьютерных систем		
3	БД	2214	Системное программирование	4	2
		2214	Основы системного программирования		
4	БД	2217	Теория вероятностей математическая статистика	4	2
		2217	Случайные процессы		
5	БД	2215	Теоретическая экономика и экономическая практика	4	2
		2215	Казахстанская модель социально-экономического развития		
6	БД	2216	Правовое и информационное обеспечение информационной безопасности	4	2
		2216	Организационное и правовое обеспечение информационной безопасности		

ТЕХНОЛОГИИ И МЕТОДЫ ПРОГРАММИРОВАНИЯ

Пререквизиты: «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования», «Основы информационной безопасности».

Постреквизиты: «Прикладное программирование», «Разработка программного обеспечения систем защиты информации», «Безопасность

Интернет-технологий», «Безопасность беспроводных сетей», «Моделирование корпоративной комплексной системы защиты информации», «Проектирование комплексных систем информационной безопасности».
Цель изучения: изучение технологий и методов программирования на основе широко используемого объектно-ориентированного языка Java и возможных уязвимостей при написании программ.
Краткое содержание дисциплины: Различные подходы к созданию программ, программирование различных структур.
Результаты изучения:
Знать: основы системного программирования, основы объектно-ориентированного подхода к программированию; методы программирования и методы разработки эффективных алгоритмов решения прикладных задач; методы отладки программ;
Уметь: оставлять, тестировать, отлаживать и оформлять программы на объектно-ориентированных языках высокого уровня;
Иметь навыки: разработки программ, по способам отладки программных комплексов.
Кафедра – Радиотехники и информационной безопасности.

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРОГРАММИРОВАНИЯ

Пререквизиты: «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования», «Основы информационной безопасности».
Постреквизиты: «Прикладное программирование», «Разработка программного обеспечения систем защиты информации», «Безопасность Интернет-технологий», «Безопасность беспроводных сетей», «Моделирование корпоративной комплексной системы защиты информации», «Проектирование комплексных систем информационной безопасности».
Цель изучения: провести анализ технологий и методов программирования на основе используемого языка программирования Java и возможных уязвимостей при написании программ.
Краткое содержание дисциплины: использовать существующие подходы к разработке программ, и способность программирования в различных структурах.
Результаты изучения:
Знать: широко применяемые основы системного программирования, использование объектно-ориентированного подхода к программированию; методы отладки программ; различные методы программирования и методы разработки эффективных алгоритмов решения прикладных задач;
Уметь: составлять и тестировать, отлаживать и оформлять программы на объектно-ориентированных языках высокого уровня;
Иметь навыки: проводить анализ программного кода и осуществлять отладку программных комплексов.
Кафедра – Радиотехники и информационной безопасности.

АРХИТЕКТУРА КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».

Постреквизиты: «Программно-аппаратные средства информационной безопасности».

Цель изучения: получение студентами знаний о внутреннем устройстве компьютерных систем с детальным изучением интерфейсов.

Краткое содержание (основные разделы): изучение базовых компонент и функций компьютерных систем, прерываний и работы с модулями ввода-вывода,системных магистралей, их функций, структурных и конструктивных особенностей, основных методов работы с внутренней и внешней памятью.

Знать:

– внутреннее устройство компьютерных систем;

Уметь:

- изменять параметры реестра Windows для проведения настройки компонентов операционной системы;

иметь навыки:

- о принципах хранения данных в реестре Windows;

Кафедра – Радиотехники и информационной безопасности.

ИНТЕРФЕЙСЫ КОМПЬЮТЕРНЫХ СИСТЕМ

Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».

Постреквизиты: «Программно-аппаратные средства информационной безопасности».

Цель изучения: знание о внутреннем устройстве компьютерных систем с детальным изучением интерфейсов.

Краткое содержание (основные разделы): исследование базовых компонент и функций компьютерных систем, прерываний и работы с модулями ввода-вывода,системных магистралей, их функций, структурных и конструктивных особенностей, основных методов работы с внутренней и внешней памятью.

Знать:

- принципы работы интерфейсов

Уметь:

- изменять параметры реестра Windows для проведения настройки компонентов операционной системы;

иметь навыки:

- о принципах хранения данных в реестре Windows;

Кафедра – Радиотехники и информационной безопасности.

СИСТЕМНОЕ ПРОГРАММИРОВАНИЕ

Пререквизиты: «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования».

Постреквизиты: «Прикладное программирование», «Разработка программного обеспечения систем защиты информации».

Цель изучения: обучение студентов основным принципам и приемам программирования на языке Ассемблера для Intel-совместимых процессоров.
Краткое содержание дисциплины: последовательно, от простого к сложному, изучить принципы проектирования программ, используя возможности технических средств ЭВМ и особенности назначения программ, включая доступ к ресурсам на физическом уровне.
Результаты изучения:
Знать: принципы проектирования программ, используя возможности технических средств ЭВМ и особенности назначения программ, включая доступ к ресурсам на физическом уровне.
Уметь: разрабатывать системы интерактивного управления вычислительным процессом с использованием элементов структурного проектирования с помощью аппаратных и программных средств.
Иметь навыки: составлять программы управления аппаратными средствами для оптимальной обработки информации, оценивать степени оптимизации программ с учётом доступа ко всем ресурсам машины.
Кафедра – Радиотехники и информационной безопасности.

ОСНОВЫ СИСТЕМНОГО ПРОГРАММИРОВАНИЯ

Пререквизиты: «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования».
Постреквизиты: «Прикладное программирование», «Разработка программного обеспечения систем защиты информации».
Цель изучения: обучение студентов основным принципам и приемам программирования на языке Ассемблера для Intel-совместимых процессоров.
Краткое содержание дисциплины: последовательно, от простого к сложному, изучить принципы проектирования программ, используя возможности технических средств ЭВМ и особенности назначения программ, включая доступ к ресурсам на физическом уровне.
Результаты изучения:
Знать: принципы проектирования программ, используя возможности технических средств ЭВМ и особенности назначения программ, включая доступ к ресурсам на физическом уровне.
Уметь: разрабатывать системы интерактивного управления вычислительным процессом с использованием элементов структурного проектирования с помощью аппаратных и программных средств.
Иметь навыки: составлять программы управления аппаратными средствами для оптимальной обработки информации, оценивать степени оптимизации программ с учётом доступа ко всем ресурсам машины.
Кафедра – Радиотехники и информационной безопасности.

ТЕОРЕТИЧЕСКАЯ ЭКОНОМИКА И ЭКОНОМИЧЕСКАЯ ПРАКТИКА

Пререквизиты: «Математика».

Постреквизиты: «Программно-аппаратные средства информационной безопасности» «Оценка рисков и аудит систем информационной безопасности».

Цель изучения: дать студентам системное, целостное представление о базовых принципах, закономерностях, механизме функционирования предприятия, обеспечить соответствующий теоретический уровень и практическую направленность в системе обучения и будущей деятельности.

Краткое содержание (основные разделы): В рамках данной дисциплины рассматриваются вопросы совершенствования методов управления, использования экономических ресурсов, методы и формы организации производства и труда, анализ финансовых результатов деятельности, вопросы развития научно-технического прогресса и оценка его эффективности.

Результаты изучения:

Знать:

– сущность экономических категорий и понятий;

– систему экономических показателей и их взаимосвязь, методы расчета этих показателей;

Уметь:

– давать правильную оценку эффективности технических решений, программных средств, систем информационной безопасности;

Иметь навыки: определять основные факторы, определяющие величину ущерба, нанесенного владельцу информации вследствие отсутствия или недостаточной надежности систем защиты информации.

Кафедра – Менеджмента и предпринимательства.

КАЗАХСТАНСКАЯ МОДЕЛЬ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОГО РАЗВИТИЯ

Пререквизиты: «Математика».

Постреквизиты: «Программно-аппаратные средства информационной безопасности» «Оценка рисков и аудит систем информационной безопасности».

Цель изучения: предоставить студентам целостное представление об основных принципах, закономерностях, механизме функционирования предприятия, а также обеспечить соответствующий теоретический уровень и практическую направленность в системе обучения и будущей деятельности.

Краткое содержание (основные разделы): рассматриваются вопросы методы и формы организации производства и труда, анализ финансовых результатов деятельности, вопросы развития научно-технического прогресса и оценка его эффективности.

Результаты изучения:

Знать:

– структуру экономических категорий и понятий;

– структуру экономических показателей и их взаимосвязь, методы расчета этих показателей;

Уметь:
– предоставлять правильную оценку эффективности технических решений, программных средств, систем информационной безопасности;

Иметь навыки: разделять существующие факторы, которые определяют размер ущерба, нанесенного собственнику информации вследствие отсутствия или недостаточной надежности систем защиты информации.

Кафедра – Менеджмента и предпринимательства.

ПРАВОВОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования», «Основы информационной безопасности».

Постреквизиты: «Программно-аппаратные средства информационной безопасности» «Оценка рисков и аудит систем информационной безопасности», «Защита баз данных», «Безопасность интернет- технологий».

Цель изучения: является изучение студентами на основе действующего законодательства и нормативно-правовой базы организационно - правового обеспечения информационной безопасности сетей и систем связи, приобретение знаний по организационному обеспечению информационной безопасности и формирование практических навыков работы по правовому обеспечению информационной безопасности.

Краткое содержание (основные разделы): организационные и информационные основы защиты и безопасности информации, отнесение сведений к конфиденциальной информации, основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации, правовая и информационное обеспечение защиты конфиденциальной информации, дисциплинарная и материальная ответственность за разглашение конфиденциальных сведений.

Результаты изучения:

Знать:

- роль и место правового обеспечения информационной безопасности сетей и систем связи в системе национальной безопасности РК;
- состояние правового обеспечения информационной безопасности РК в области использования информационной инфраструктуры и информационных ресурсов, инфокоммуникационных систем и сетей связи;
- назначение и место правовой защиты информации в информационной безопасности сетей и систем связи;
- основные направления совершенствования правового обеспечения информационной безопасности сетей и систем связи; меры гражданско-правовой, уголовной, административной и дисциплинарной ответственности за разглашение защищаемой информации и нарушение правил её защиты;
- теоретические основы функционирования систем организационного обеспечения информационной безопасности сетей и систем связи, ее современные проблемы и терминологию;

- основные направления и методы организационной защиты информации в сетях и системах связи.

Уметь:

- применять нормативно-правовые акты в области обеспечения информационной безопасности сетей и систем связи с целью создания новых перспективных систем защиты инфокоммуникаций;
- анализировать эффективность систем организационной защиты информации сетей и систем связи и разрабатывать направления ее развития;
- использовать нормативную и правовую документацию, характерную для информационной безопасности и методологии защиты инфокоммуникаций (законы РК, технические регламенты, международные и национальные стандарты, рекомендации МСЭ, стандарты связи, протоколы, терминологию);
- изучать научно-техническую информацию, отечественный и зарубежный опыт в области организационно правового обеспечения информационной безопасности сетей и систем связи;

Иметь навыки: обеспечение защиты конфиденциальной информации

Кафедра – Радиотехники и информационной безопасности.

ОРГАНИЗАЦИННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования», «Основы информационной безопасности».

Постреквизиты: «Программно-аппаратные средства информационной безопасности» «Оценка рисков и аудит систем информационной безопасности», «Защита баз данных», «Безопасность интернет- технологий».

Цель изучения: является изучение студентами на основе действующего законодательства и нормативно-правовой базы организационно - правового обеспечения информационной безопасности сетей и систем связи, приобретение знаний по организационному обеспечению информационной безопасности и формирование практических навыков работы по правовому обеспечению информационной безопасности.

Краткое содержание (основные разделы): организационные и информационные основы защиты и безопасности информации, отнесение сведений к конфиденциальной информации, основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации, правовая и информационное обеспечение защиты конфиденциальной информации, дисциплинарная и материальная ответственность за разглашение конфиденциальных сведений.

Результаты изучения:

Знать:

- роль и место правового обеспечения информационной безопасности сетей и систем связи в системе национальной безопасности РК;

- состояние правового обеспечения информационной безопасности РК в области использования информационной инфраструктуры и информационных ресурсов, инфокоммуникационных систем и сетей связи;
- назначение и место правовой защиты информации в информационной безопасности сетей и систем связи;
- основные направления совершенствования правового обеспечения информационной безопасности сетей и систем связи; меры гражданско-правовой, уголовной, административной и дисциплинарной ответственности за разглашение защищаемой информации и нарушение правил её защиты;
- теоретические основы функционирования систем организационного обеспечения информационной безопасности сетей и систем связи, ее современные проблемы и терминологию;
- основные направления и методы организационной защиты информации в сетях и системах связи.

Уметь:
- применять нормативно-правовые акты в области обеспечения информационной безопасности сетей и систем связи с целью создания новых перспективных систем защиты инфокоммуникаций;
- анализировать эффективность систем организационной защиты информации сетей и систем связи и разрабатывать направления ее развития;
- использовать нормативную и правовую документацию, характерную для информационной безопасности и методологии защиты инфокоммуникаций (законы РК, технические регламенты, международные и национальные стандарты, рекомендации МСЭ, стандарты связи, протоколы, терминологию);
- изучать научно-техническую информацию, отечественный и зарубежный опыт в области организационно правового обеспечения информационной безопасности сетей и систем связи;

Иметь навыки: обеспечение защиты конфиденциальной информации
Кафедра – Радиотехники и информационной безопасности.

ТЕОРИЯ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧЕСКАЯ СТАТИСТИКА

Пререквизиты: «Информационно-коммуникационные технологии», «Математика».
Постреквизиты: «Безопасность и администрирование систем и сетей».
Цель изучения: освоение современных математических методов для решения прикладных задач
Краткое содержание (основные разделы): Случайные события и случайные величины. Основные распределения, используемые в радиотехнике и связи и их числовые характеристики. Случайные многомерные величины. Предельные теоремы. Случайный процесс. Математическая статистика.
Результаты изучения:
Знать: основные законы распределений случайных величин и их числовые параметры, способы обработки информации, их систематизации и методы анализа статистических данных;

Уметь: ставить задачи, строить математические модели,применять современные компьютерные программы в решении математических задач с использованием аналитических и численных методов, определять неизвестные параметры распределений случайных величин через оценку, находить числовые характеристики по выборочным статистическим данным при исследовании процессов в управлении;

Иметь навыки − решения инженерных задач с применением математических методов.

Кафедра – Математического моделирования и программного обеспечения.

СЛУЧАЙНЫЕ ПРОЦЕССЫ

Пререквизиты: «Информационно-коммуникационные технологии», «Математика».

Постреквизиты: «Безопасность и администрирование систем и сетей».

Цель изучения: освоение современных математических методов для решения прикладных задач

Краткое содержание (основные разделы): Случайные события и случайные величины. Случайный процесс. Проверка статистических гипотез. Корреляционная зависимость.

Результаты изучения:

Знать: теоремы сложения и умножения вероятностей случайных событий, законы распределения вероятностей случайных величин, числовые характеристики случайных величин, числовые характеристики случайной двумерной величины, интервальные оценки параметров**;**

Уметь: использовать теорию случайных процессов для решения прикладных задач, использовать теоретический закон распределения по данному вариационному ряду;

Иметь навыки − решения инженерных задач с применением математических методов.

Кафедра – Математического моделирования и программного обеспечаения.

№ п/п	Цикл дисциплин	Цифровой код дисциплин	Наименование дисциплины	Семестр	Кол-во кредитов
1	БД	3218	Безопасность Web-приложений	5	2
		3218	Организация безопасности порталов		
2	БД	3219	Программирование на языках высокого уровня	5	3
		3219	Скриптовые языки		
3	БД	3220	Микроконтроллеры и их применение в информационной безопасности	5	2

		3220	Микроконтроллеры и микропрограммирование		
4	БД	3221	Организация вычислительных систем и сетей	5	3
		3221	Сети и системы передачи информации		
5	БД	3222	Криптографические методы и средства защиты информаций	5	3
		3222	Криптографические методы информационной безопасности		
6	БД	3228	Компьютерная аналитика	5	3
		3228	Социальная инженерия в аспекте информационной безопасности		
7	БД	3224	Стандартизация и сертификация средств информационной безопасности	5	2
		3224	Стандартизация систем информационной безопасности		
8	ПД	3303	Прикладное программирование	6	3
		3303	Разработка программного обеспечения систем защиты информации		
9	ПД	3304	Технические средства защиты информации	6	3
		3304	Технические средства противодействия радиоразведкам		
10	ПД	3305	Программно-аппаратные средства информационной безопасности	6	3
		3305	Информационная безопасность программно-прикладных средств		
11	БД	3225	Основы систем баз данных	6	3
		3225	Проектирование баз данных		
12	БД	3226	Безопасность Интернет-технологий	6	3
		3226	Безопасность беспроводных сетей		
13	БД	3227	Администрирование доменных систем	6	3
		3227	Администрирование информационных систем		

БЕЗОПАСНОСТЬ WEB-ПРИЛОЖЕНИЙ

Пререквизиты: «Операционная система Linux», «Информационно-коммуникационные технологии».

Постреквизиты: «Безопасность Интернет-технологий», «Безопасность беспроводных сетей».
Цель изучения: освоение технологий, принципов организации и функционирования защищенных WEB-приложений, обучение методам проектирования серверных приложений для использования в среде Интернет.
Краткое содержание (основные разделы): обзор WEB-технологий; знакомство с механизмом работы WEB-серверов; изучение технологии создания серверных WEB-приложений; изучение технологии создания клиентских WEB-приложений; приобретение навыков программирования с помощью скриптового языка PHP; рассмотрение перспектив развития WEB.
Результаты изучения:
уметь: создавать серверные приложения на основе современных WEB-технологий;
знать: принципы технологии для реализации WEB-проектов любого назначения; основы проектирования и защиты информационных систем; системы и модели обработки информации; управлять базами данных; серверный язык программирования PHP;
иметь навыки: проектирования и реализации защищенных WEB-проектов.
Кафедра – Радиотехники и информационной безопасности.

ОРГАНИЗАЦИЯ БЕЗОПАСНОСТИ ПОРТАЛОВ

Пререквизиты: «Операционная система Linux», «Информационно-коммуникационные технологии».
Постреквизиты: «Безопасность Интернет-технологий», «Безопасность беспроводных сетей».
Цель изучения: освоение технологий, принципов организации и функционирования защищенных WEB-приложений, обучение методам проектирования серверных приложений для использования в среде Интернет.
Краткое содержание (основные разделы): обзор WEB-технологий; знакомство с механизмом работы WEB-серверов; изучение технологии создания серверных WEB-приложений; изучение технологии создания клиентских WEB-приложений; приобретение навыков программирования с помощью скриптового языка PHP; рассмотрение перспектив развития WEB.
Результаты изучения:
уметь: создавать серверные приложения на основе современных WEB-технологий;
знать: принципы технологии для реализации WEB-проектов любого назначения; основы проектирования и защиты информационных систем; системы и модели обработки информации; управлять базами данных; серверный язык программирования PHP;
иметь навыки: проектирования и реализации защищенных WEB-проектов.
Кафедра – Радиотехники и информационной безопасности.

ПРОГРАММИРОВАНИЕ НА ЯЗЫКАХ ВЫСОКОГО УРОВНЯ

Пререквизиты: «Информационно-коммуникационные технологии», «Математика», «Алгоритмизация и языки программирования», «Технологии и методы программирования», «Методологические основы программирования».

Постреквизиты: «Прикладное программирование», «Разработка программного обеспечения систем защиты информации», «Программно-аппаратные средства информационной безопасности», «Информационная безопасность программно-прикладных средств.

Цель изучения: подготовка студентов к эффективному использованию современной компьютерной техники при решении задач программирования посредством изучения языка высокого уровня Python, в освоении студентами методов и средств, а также основ программирования и подготовка к их активному их использованию в выбранной специальности.

Краткое содержание (основные разделы): Дисциплина служит для освоения фундамента программирования в современных информационных технологий и компьютерных азов студентами и приобретению ими навыков и умения целенаправленно использовать их в своей практической работе. Это связано с тем, что компьютеры и компьютерные технологии внедряются и используются во всех сферах деятельности человека, где бы он ни работал.

Результаты изучения:

Знать:

- основные понятия и основные структуры языка программирования Python;
- особенности, принципы алгоритмизации и реализацию алгоритмов в Python;
- наиболее часто встречающимися структуры данных, уметь ими пользоваться и знать внутреннюю организацию;
- об особенностях и последних достижениях в области разработки кроссплатформенного ПО;
- о положительных и отрицательных чертах подхода к ООП программированию;
- основы технологий объектного программирования.

Уметь:

- разрабатывать алгоритмы и создавать программы на языке программирования высокого уровня;
- знать технологию создания консольных и оконных приложений.

Иметь навыки:

разработки программ в среде Java (Python), объектного программирования, создания программ начиная от консольных приложений, заканчивая приложениями для работы с базами данных и Internet.

Кафедра – Радиотехники и информационной безопасности.

СКРИПТОВЫЕ ЯЗЫКИ

Пререквизиты: «Информационно-коммуникационные технологии», «Математика», «Алгоритмизация и языки программирования», «Технологии и методы программирования», «Методологические основы программирования».

Постреквизиты: «Прикладное программирование», «Разработка программного обеспечения систем защиты информации», «Программно-аппаратные средства информационной безопасности», «Информационная безопасность программно-прикладных средств».

Цель изучения: подготовка студентов к эффективному использованию современной компьютерной техники при решении задач программирования посредством изучения языка высокого уровня Java, в освоении студентами методов и средств, а также основ программирования и подготовка к их активному их использованию в выбранной специальности.

Краткое содержание (основные разделы): Дисциплина служит для освоения фундамента программирования в современных информационных технологий и компьютерных азов студентами и приобретению ими навыков и умения целенаправленно использовать их в своей практической работе. Это связано с тем, что компьютеры и компьютерные технологии внедряются и используются во всех сферах деятельности человека, где бы он ни работал.

Результаты изучения:

Знать:

- основные понятия и основные структуры языка программирования Java;
- особенности, принципы алгоритмизации и реализацию алгоритмов в Java;
- наиболее часто встречающимися структуры данных, уметь ими пользоваться и знать внутреннюю организацию;
- об особенностях и последних достижениях в области разработки кроссплатформенного ПО;
- о положительных и отрицательных чертах подхода к ООП программированию;
- основы технологий объектного программирования.

Уметь:

- разрабатывать алгоритмы и создавать программы на языке программирования высокого уровня;
- знать технологию создания консольных и оконных приложений.

Иметь навыки:

разработки программ в среде Java, объектного программирования, создания программ начиная от консольных приложений, заканчивая приложениями для работы с базами данных и Internet.

Кафедра – Радиотехники и информационной безопасности.

МИКРОКОНТРОЛЛЕРЫ И ИХ ПРИМЕНЕНИЕ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Математика», «Физика».

Постреквизиты: «Прикладное программирование», «Разработка программного обеспечения систем защиты информации».

Цель изучения: изучить свойства и характеристики AVR микроконтроллеров, элементы памяти, индикации и исполнительных устройств системы управления, а также алгоритмические языки программирования микроконтроллеров (ассемблер, Си).

Краткое содержание (основные разделы): современные и перспективные направления развития цифровых систем, области применения различных цифровых систем управления и контроля, принцип действия и конструктивные особенности электронных приборов, структура и характеристики AVR микроконтроллеров, принципы программирования микроконтроллеров на языке ассемблер и Си.

Результаты изучения:

Знать: принцип действия и конструктивные особенности электронных приборов; архитектуру и команды AVR микроконтроллеров; структуру и функциональные возможности микроконтроллеров и периферийных устройств; алгоритмические языки программирования микроконтроллеров (ассемблер, Си).

Уметь: программировать микроконтроллеры на языках Си и ассемблер; оценивать эффективность и выбирать тип микроконтроллера для конкретных систем; производить предварительный расчет параметров и выбор основных элементов цифровой системы управления и контроля.

иметь навыки: осуществлять «прошивку» микроконтроллеров машинным кодом; программировать микроконтроллеры; производить предварительный расчет параметров и выбор основных элементов цифровой системы управления.

Кафедра – Электроники и робототехники.

МИКРОКОНТРОЛЛЕРЫ И МИКРОПРОГРАММИРОВАНИЕ

Пререквизиты: «Математика», «Физика».

Постреквизиты: «Прикладное программирование», «Разработка программного обеспечения систем защиты информации».

Цель изучения: изучить свойства и характеристики различных типов микроконтроллеров (AVR, PIC), элементы индикации и исполнительных устройств системы управления, а также алгоритмический язык ассемблер для программирования микроконтроллеров.

Краткое содержание (основные разделы): современные и перспективные направления развития цифровых систем, области применения различных цифровых систем управления и контроля, принцип действия и конструктивные особенности электронных приборов, структура и характеристики различных типов микроконтроллеров, принципы программирования микроконтроллеров на языке ассемблер.

Результаты изучения:

Знать: архитектуру, структуру и команды AVR микроконтроллеров; архитектуру, структуру и команды PIC микроконтроллеров; алгоритмические языки программирования: ассемблер для AVR микроконтроллеров, ассемблер для PIC микроконтроллеров.

уметь: оценивать эффективность и выбирать тип микроконтроллера для конкретных систем; осуществлять «прошивку» микроконтроллеров машинным кодом; производить предварительный расчет параметров и выбор основных элементов цифровой системы управления и контроля.

иметь навыки: программировать микроконтроллеры на языке ассемблер; осуществлять выбор основных элементов цифровой системы управления.
Кафедра – Электроники и робототехники.

ОРГАНИЗАЦИЯ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И СЕТЕЙ

Пререквизиты: «Информационно-коммуникационные технологии», «Физика», «Операционная система Linux».
Постреквизиты: «Безопасность и администрирование систем и сетей», «Программно-аппаратные средства информационной безопасности».
Цель изучения: дисциплины «организация вычислительных систем и сетей» является изучение особенностей организации вычислительных машин, систем и сетей ЭВМ, принципов построения отдельных устройств и взаимодействия их в процессе ввода, обработки и вывода информации.
Краткое содержание (основные разделы): принципы организации и функционирования вычислительных систем и сетей, особенности работы персонального компьютера в сетях, современные компьютерные сетевые технологии и способами передачи, хранения, поиска, обработки и представления информации, технология Интернет.
Результаты изучения:
Знать: в процессе изучения курса студенты должны получить систематизированные знания об организации и основных принципах работы узлов и устройств ЭВМ в частности и вычислительных систем и сетей в целом. Также должен понимать работу стека протоколов TCP/IP и разбираться в назначений каждого уровня модели OSI.
Уметь: пользоваться средствами вычислительных систем и сетей, понимать особенности структурной организации и программного обеспечения средств вычислительной техники, владеть принципами модернизации средств вычислительной техники. Классифицировать сеть по способу передачи данных и произвести тестирование и сертификацию кабельной системы с помощью специализированных приборов.
иметь навыки: по установке и конфигурированию компонентов компьютерных систем и драйвера сетевых плат для различной среды передачи данных; по построению локальных сетей небольшого размера; определять современные методы обеспечения отказоустойчивости компьютерных и коммуникационных систем; по конфигурированию сети с несколькими маршрутизаторами. Поднимать протоколы маршрутизаций для сети корпораций.
Кафедра – Радиотехники и информационной безопасности.

СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Пререквизиты: «Информационно-коммуникационные технологии», «Физика», «Операционная система Linux».
Постреквизиты: «Безопасность и администрирование систем и сетей», «Программно-аппаратные средства информационной безопасности».

Цель изучения – дисциплины «Сети и системы передачи информации» является изучение студентами базовых понятий в области телекоммуникационных технологий и освоение ими методов постановки, подготовки и решения научных, инженерно-технических и экономических задач в области телекоммуникаций с использованием современных информационных технологий.

Краткое содержание (основные разделы): В ходе преподавания дисциплины изучаются принципы построения современных систем и сетей связи. Знакомство с основными определениями и классификацией систем и сетей связи, изучение модели взаимодействия открытых систем, изучение структуры и функций территориальных сетей. Даются определения технологии локальных сетей, технологии глобальных инфокоммуникационных систем, модель OSI и адресация в современных сетях, типы протоколов в компьютерных системах и сетях, стек TCP/IP, виртуальные локальные сети.

Результаты изучения:

Знать: способы представления информации, её преобразования, современные способы получения, хранения и выдачи цифровой информации применительно к инфокоммуникационным системам и сетям; современную нормативную и правовую документацию в области инфокоммуникационных технологий и систем связи, включая рекомендации Международного союза электросвязи, стандарты связи, протоколы; современные методы управления потоками трафика в инфокоммуникационных системах и сетях и методы проведения испытаний; источники современной научно-технической информации способы её анализа;

Уметь: собирать и анализировать информацию для формирования исходных данных для проектирования инфокоммуникационных систем и сетей; применять на практике научно-техническую информацию, отечественный и зарубежный опыт при разработке и эксплуатации инфокоммуникационных систем и сетей; составлять нормативную документацию (инструкции) по эксплуатационно-техническому обслуживанию инфокоммуникационных систем; использовать нормативную и правовую документацию, характерную для области инфокоммуникационных технологий и систем связи; внедрять перспективные технологии и стандарты.

иметь навыки: по работе с основными методами и средствами получения, хранения, переработки информации в инфокоммуникационных системах; навыками выбора структуры инфокоммуникационных систем и сетей и анализа информационных процессов и потоков в этих системах, способами моделирования информационных процессов в инфокоммуникационных системах и сетях; навыками проектирования инфокоммуникационных систем и сетей с использованием передового мирового опыта.

Кафедра – Радиотехники и информационной безопасности.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Пререквизиты: «Информационно-коммуникационные технологии», «Математика», «Основы информационной безопасности».

Постреквизиты: «Проектирование комплексных систем информационной безопасности», «Системы видеонаблюдения и контроля доступа.

Цель изучения:

- формирование у студентов знаний по основам построения и практического применения защиты информации в инфо-коммуникационных системах. и формирование у будущих специалистов систематизированных знаний о принципах, методах и средствах защиты информации при ее передаче,
- прогнозирование ситуаций и принятие грамотных мер для решений в разных условиях и ситуациях по защите информации в локальных и глобальных вычислительных сетях,
- применение новейших средств и методов защиты информации в различных технологиях при ее передаче по сетям.

Краткое содержание (основные разделы): ставит целью, дать будующим специалистам сведения об организационных, административных, технических, программных и алгоритмических методах и средствах защиты компьютерной информации в компьютерных сетях и системах для области инфо-коммуникационной безопасности.

Результаты изучения:

Знать: основные принципы защиты информации в инфо-коммуникационных системах; основные методы оценки защиты информации в инфо-коммуникационных системах; основные приемы проведения методов защиты в инфо-коммуникационных сетях, прогноза ее состояния в области мониторинга и ее анализа для принятия решения;

Уметь: защищать информацию в инфо-коммуникационных сетях при её передачи; применять методы по выбору наилучшего кода шифрования и осуществлять сравнительный анализ, организовывать и проводить мнроприятия по защите информации в инфо-коммуникационных сетях. Конфигурировать параметры аутентификации и параметры безопасности подсоединения системы к глобальным сетям. Администрирование средств защиты компьютерной сети. Применение средств шифрования, уметь планировать политику безопасности.

Иметь навыки: производить анализ показателей качества и критерия оценки безопасности систем, методов и средств защиты информации.

Кафедра – Радиотехники и информационной безопасности.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Информационно-коммуникационные технологии», «Математика», «Основы информационной безопасности».

Постреквизиты: «Проектирование комплексных систем информационной безопасности», «Системы видеонаблюдения и контроля доступа.

Цель изучения:
- формирование у студентов знаний по теоретическим основам построения и практического применения систем защиты информации в инфо-коммуникационных системах. и формирование у будущих специалистов систематизированного представления о принципах, методах и средствах реализации защиты данных при ее передаче,
- прогнозирование и принятия грамотных решений в условиях чрезвычайных ситуаций по защите информации в локальных и глобальных инфо-коммуникационных сетях,
- применение современных средств и методов защиты информации в различных технологиях при ее передаче.

Краткое содержание (основные разделы): ставит целью, дать студентам систематизированные сведения об организационных, административных, технических, программных и алгоритмических методах и средствах защиты компьютерной информации в компьютерных системах и сетях в области инфо-коммуникационной безопасности.

Результаты изучения: Знать: основы защиты информации в инфо-коммуникационных системах; методы оценки защиты информации в инфо-коммуникационных системах; приемы проведения в области инфо-коммуникационных сетей, прогноза ее состояния в области мониторинга и ее анализа для принятия оптимального решения;

Уметь: обеспечивать защиту информации в инфо-коммуникационных сетях в процессе передачи информации; разрабатывать методы по выбору наилучшего кода шифрования и осуществлять сравнительный анализ организовывать и проводить проверку знаний по защите информации в инфо-коммуникационных сетях. Конфигурировать параметры аутентификации и параметры безопасности подсоединения системы к глобальным сетям. Администрированием средств защиты компьютерной сети. Использованием средств шифрования, планировать политику безопасности.

Иметь навыки: производить выбор и анализ показателей качества и критерия оценки систем, отдельных методов и средств защиты информации.

Кафедра – Радиотехники и информационной безопасности.

КОМПЬЮТЕРНАЯ АНАЛИТИКА

Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».

Постреквизиты: «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях», «Защита информации от программных угроз и несанкционированного доступа мобильных устройств».

Цель изучения: формирование системы теоретических знаний и практических навыков в области компьютерной аналитики.

Краткое содержание (основные разделы): изучение общих принципов выявления угроз информационной безопасности объектов, и разработка методов противодействия им. А также организация работ коллектива

исполнителей, принимать управленческие решения в условиях спектра мнений, определять порядок выполнения работ.

Результаты изучения:

Знать:

- основы организации и функционирования сетей;
- основные методы и средства анализа информационных атак;
- базовые технологии обеспечения защиты и безопасности информации в беспроводных сетях;
- основные практические направления построения систем защиты и безопасности беспроводных сетей.

Уметь:

- использовать в практической деятельности существующие методы и средства контроля и защиты информации в телекоммуникационных сетях;
- применять средства анализа защищенности обнаружения атак в информационных сетях;
- организовать практическую защиту информации в сетях связи;

Иметь навыки: по применению технических и программных средств обеспечения безопасности информационных сетей.

Кафедра – Радиотехники и информационной безопасности.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В АСПЕКТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».

Постреквизиты: «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях», «Защита информации от программных угроз и несанкционированного доступа мобильных устройств».

Цель изучения: формирование у студентов знаний и умений использования средств защиты информации и их практического применения для организации систем защиты современных информационных сетей.

Краткое содержание (основные разделы): изучение общих принципов организации и функционирования информационных сетей, современных средств анализа и обнаружения информационных атак и методов защиты информации. А также рассматриваются основные протоколы, применяемые для обеспечения безопасности информационных сетей.

Результаты изучения:

Знать:

- основы организации и функционирования информационных сетей;
- основные методы и средства анализа информационных атак;
- базовые технологии обеспечения защиты и безопасности информации в Сетях связи;
- основные практические направления построения систем защиты и безопасности информационных сетей.

Уметь:

- использовать в практической деятельности существующие методы и

средства контроля и защиты информации в информационных сетях;
- применять средства анализа защищенности обнаружения атак в информационных сетях;
- организовать практическую защиту информации в сетях связи;
Иметь навыки: по применению технических и программных средств обеспечения безопасности беспроводных сетей.
Кафедра – Радиотехники и информационной безопасности.

СТАНДАРТИЗАЦИЯ И СЕРТИФИКАЦИЯ СРЕДСТВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Математика», «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования», «Основы информационной безопасности».
Постреквизиты: «Программно-аппаратные средства информационной безопасности», «Защита баз данных», «Безопасность интернет технологий».
Цель изучения: ознакомить студентов с критериями установления оптимального уровня упорядочения и унификации, обеспечения взаимозаменяемости продуктов ИБ, а также измеримости и повторяемости результатов.
Краткое содержание (основные разделы): Основными задачами дисциплины является формирование у студентов теоретических знаний и практических навыков по проблемам технологии разработки и использования средств информационной безопасности, оценки качества и повышения надёжности.
Результаты изучения:
знать:
- основные стандарты и сертификаты;
- состояние экспертных систем в области использования информационной инфраструктуры и информационных ресурсов, инфокоммуникационных систем и сетей связи;
- назначение и место стандартизации и сертификации средств информационной безопасности сетей и систем связи;
Уметь:
- разрабатывать в соответствии с ГОСТами пояснительную записку, техническое задание на разработку средств информационной безопасности;
- анализировать эффективность средств информационной безопасности и определение их задачи функций;
Иметь навыки: применения основных стандартов информационной безопасности
Кафедра – Радиотехники и информационной безопасности.

СТАНДАРТИЗАЦИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Математика», «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования», «Основы информационной безопасности».

Постреквизиты: «Программно-аппаратные средства информационной безопасности», «Защита баз данных», «Безопасность интернет технологий».

Цель изучения: ознакомить студентов с обеспечением взаимозаменяемости продуктов информационной безопасности, с критериями установления оптимального уровня упорядочения и унификации,

Краткое содержание (основные разделы): формирование у студентов теоретических знаний и практических навыков по проблемам технологии разработки и использования средств информационной безопасности, оценки качества и повышения надёжности.

Результаты изучения: о методах оценки информационных и экономических показателей эффективности сложных профессионально-ориентированных систем, о стандартизации и сертификации в области информационных технологий; о современных международных стандартах; о сертификации.

знать:

- существующие стандарты и сертификаты;
- текущее положение экспертных систем в области использования информационной инфраструктуры инфокоммуникационных систем и сетей связи и информационных ресурсов;
- в информационной безопасности сетей и систем связи осуществление назначения и место стандартизации и сертификации средств;

Уметь:

- применять научно-техническую информацию, отечественный и зарубежный опыт в области стандартизации и сертификации для определения критериев оценки средств информационной безопасности;
- пользоваться нормативной и правовой документацией, характерную для информационной безопасности и методологии защиты инфокоммуникаций (законы РК, технические регламенты, международные и национальные стандарты, сертификаты, рекомендации МСЭ, стандарты связи, протоколы, терминологию);
- разрабатывать техническое задание на разработку средств информационной безопасности в соответствии с ГОСТами пояснительную записку.

Иметь навыки: применения основных стандартов информационной безопасности

Кафедра – Радиотехники и информационной безопасности.

ПРИКЛАДНОЕ ПРОГРАММИРОВАНИЕ

Пререквизиты: «Информационно-коммуникационные технологии», «Математика», «Программирование на языках высокого уровня».

Постреквизиты: «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях», «Защита информации от программных угроз и несанкционированного доступа мобильных устройств».
Цель изучения: изучение способов разработки программ, средств защиты программ, а также овладение необходимыми знаниями и навыками по разработке приложений для разрабатываемых программ. Полученные знания и навыки могут быть использованы студентами в течение дальнейшего процесса обучения, заканчивая написанием приложения к дипломному проекту.
Краткое содержание (основные разделы): Дисциплина является естественно-научной дисциплиной, включающей в себя решение математических и инженерно-технических задач и математического моделирования, алгоритмизации в области информационных систем и возможность их развития в других дисциплинах при реализации концепции защиты от взлома в области прикладных инженерных задач.
Результаты изучения:
- объектную структуру и набор программных средств как класса программного обеспечения;
- конструктивное наполнение программных продуктов;
- возможные способы управления и организации интерфейсного взаимодействия с иными приложениями;
- возможные «наполнители» алгоритмических конструкций;
- операторы, типы данных, возможности языка программирования.

уметь:
- использовать интерфейсный подход создания программных средств;
- использовать интерфейсный подход к созданию взаимодействия внутренних данных с внешними приложениями;
- определить задачи с использованием знания о возможностях решения конкретных задач;
- использовать среду отладки и грамотно отслеживать этажность и специфику ошибок.

иметь навыки:
- разработки приложений;
- покомпонентной отладки программ;

Кафедра – Радиотехники и информационной безопасности.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Пререквизиты: «Информационно-коммуникационные технологии», «Математика», «Программирование на языках высокого уровня».
Постреквизиты: «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях», «Защита информации от программных угроз и несанкционированного доступа мобильных устройств».
Цель изучения: изучение основ технологий и методов разработки программного обеспечения, средств защиты программного обеспечения, а

также овладение необходимыми знаниями и навыками по разработке приложений для прикладных пакетов. Полученные знания и навыки могут быть использованы студентами в течение дальнейшего процесса обучения, заканчивая написанием приложения к дипломному проекту.

Краткое содержание (основные разделы): Дисциплина является естественно-научной дисциплиной, включающей в себя решение математических и инженерно-технических задач и математического моделирования, алгоритмизации в области информационных систем и возможность их развития в других дисциплинах при реализации концепции защиты от взлома в области прикладных инженерных задач.

Результаты изучения:

знать:

- структуру и состав пакета прикладных программ как класса программного обеспечения;
- функциональное назначение основных компонентов прикладного пакета;
- синтаксические конструкции встроенного языка программирования, операторы, используемые типы данных, возможности языка программирования;
- объектно-ориентированные возможности пакетов;
- способы организации взаимодействия с внешними приложениями.

уметь:

- формулировать прикладные задачи в терминах предметной области пакета прикладных программ;
- использовать предоставляемые прикладным пакетом возможности для решения конкретных задач;
- использовать интегрированные средства отладки и профилирования приложений.

Иметь навыки:

- о принципах работы компонентов пакета прикладных программ;
- тенденциях в развитии пакета прикладных программ.

Кафедра – Радиотехники и информационной безопасности.

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Пререквизиты: «Информационно-коммуникационные технологии», «Физика», «Операционная система Linux».

Постреквизиты: «Системы видеонаблюдения и контроля доступа».

Цель изучения: формирование у студентов общих понятий о принципах работы и характеристиках современных средств защиты информации. Такая цель обусловлена несколькими причинами. Во-первых, защита от утечки информации является основой нормального функционирования любой системы, занимающейся обработкой информации. Во-вторых, правильное использование технических средств защиты позволяет предотвратить материальные и интеллектуальные потери предприятия.

Краткое содержание (основные разделы):

– изучение студентом основных понятий ТСЗИ,

– изучение студентом технических каналов утечки информации;
– изучение студентом понятия о поиске и обнаружении ТКУИ;
– умение обнаружить имеющиеся каналы утечки информации;
– умение работать с техническими средствами защиты информации
- иметь представления об использовании технических средств защиты информации и применять полученные навыки в практической деятельности специалиста по техническим средствам защиты информации.

Результаты изучения:

Знать:

– методы и средства выявления угроз безопасности;
– методы технической защиты информации;
– методы формирования требований по защите информации;
– методы расчета и контроля показателей технической защиты информации;
– методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов 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:

– исследовать технические каналы на возможность утечки информации;
– проверить каждый канал на наличие технических средств съема информации;
– работать с поисковыми техническими средствами ;
– применять методы проведения поисковых мероприятий на практических примерах
– иметь представления о современных поисковых средствах и средствах защиты и применять полученные навыки в практической деятельности специалиста по техническим средствам защиты информации.

Иметь навыки: по техническому контролю эффективности принимаемых мер защиты; защиты технических средств передачи, обработки и хранения информации.

Кафедра – Радиотехники и информационной безопасности.

ТЕХНИЧЕСКИЕ СРЕДСТВА ПРОТИВОДЕЙСТВИЯ РАДИОРАЗВЕДКАМ

Пререквизиты: «Информационно-коммуникационные технологии», «Физика», «Операционная система Linux».

Постреквизиты: «Системы видеонаблюдения и контроля доступа».

Цель изучения: формирование у студентов общих понятий о принципах работы и характеристиках современных средств защиты информации. Такая цель обусловлена несколькими причинами. Во-первых, защита от утечки информации является основой нормального функционирования любой

системы, занимающейся обработкой информации. Во-вторых, правильное использование технических средств защиты позволяет предотвратить материальные и интеллектуальные потери предприятия.

Краткое содержание (основные разделы):

– изучение студентом основных понятий разведки,
– изучение студентом технических каналов утечки информации;
– изучение студентом понятия о поиске и обнаружении ТКУИ;
– практическое умение в проведении поисковых мероприятий;
– практическое умение работать со средствами защиты информации
- применять полученные навыки в практической деятельности специалиста по техническим средствам защиты информации.

Результаты изучения:

Знать:

– методы и средства разведки;
– методы применения технических средств защиты информации;
– методы формирования требований по защите информации;
– методы расчета и контроля показателей технической защиты информации;
– методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов технические каналы утечки информации;
– способы и средства защиты информации от утечки по техническим каналам,
– методы и средства контроля эффективности технической защиты информации;

Уметь:

– исследовать возможность утечки информации через технические каналы;
– проверить наличие технических средств съема информации в каждом канале
– работать со всеми возможными техническими средствами проведения проверочных мероприятий;
– применять методы проведения поисковых мероприятий на практических примерах
– применять полученные навыки в практической деятельности специалиста по техническим средствам защиты информации.

Иметь навыки: по методике расчета эффективности принимаемых мер защиты; защиты технических средств передачи, обработки и хранения информации.

Кафедра – Радиотехники и информационной безопасности.

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».

Постреквизиты: «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях», «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях».
Цель изучения: приобретение студентами основополагающих знаний об основных принципах защиты информации, а также обеспечения безопасности информации. Дается толкование основных понятий: криптография, конфиденциальность, целостность, аутентификация, цифровая подпись.
Краткое содержание (основные разделы): программно-технические средства защиты объекта, методы и средства привязки программного обеспечения к техническому окружению и физическим носителям, методы и средства хранения ключевой информации, защита программ от излучения и от разрушающих программных воздействий, системные вопросы защиты программ и данных.
Результаты изучения:
Знать:
-базовые технологии обеспечения безопасности в информационных системах, их возможности;
- основные методы защиты информации в информационных системах.
Уметь:
- обеспечивать безопасность и защиту информации в процессе передачи информации;
- применять методы по выбору наилучшего способа обеспечения защиты информации в информационных системах;
- организовывать и проводить проверку знаний по защите информации в информационных системах.
Иметь навыки: по современным аппаратнымм средствам защиты систем ЭВМ.
Кафедра – Радиотехники и информационной безопасности.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОГРАММНО-ПРИКЛАДНЫХ СРЕДСТВ
Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».
Постреквизиты: «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях», «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях».
Цель изучения: приобретение студентами основных знаний о принципах организации информационной безопасности, а также обеспечения безопасности программно-прикладных средств. Дается разъяснение основных понятий: аутентификация, электронные ключи, программные защитные механизмы, аппаратные защитные механизмы
Краткое содержание (основные разделы): основы системы безопасности и методы защиты информации в прикладных системах, методы оценки защиты информации в прикладных системах, а так же ознакомление со средствами обеспечения прикладных систем от потери информации, ознакомление с

возможностью прогноза состояния систем безопасности и их анализа для принятия оптимального решения по обеспечению защиты информации в прикладных системах.

Результаты изучения:

Знать:

- основные технологии обеспечения информационной безопасности в прикладных системах, их возможности;
- основные методы обеспечения безопасности программно-прикладных средств.

Уметь:

- обеспечивать защиту от несанкционированного доступа и сетевых хакерских атак;
- применять средства по выбору лучшего способа обеспечения информационной безопасности в прикладных системах;
- проводить исследование и настройку систем обнаружения вторжений в прикладных системах.

Иметь навыки: по современным прикладным средствам защиты систем ЭВМ.

Кафедра – Радиотехники и информационной безопасности.

ОСНОВЫ СИСТЕМ БАЗ ДАННЫХ

Пререквизиты: «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования», «Программирование на языках высокого уровня», «Технологии и методы программирования».

Постреквизиты: «Защита баз данных».

Цель изучения: формирование у студентов общих понятий о системах баз данных, архитектуры систем баз данных; понятий реляционной модели, основных элементов стандартного реляционного языка SQL; умение создать реальную базу данных; умение работать в сетевой или локальной базе данных, изучение принципов построения основных моделей данных и их использование в современных системах управления базами данных (СУБД), изучение методов защиты и безопасности баз данных.

Краткое содержание (основные разделы): основные понятия распределенных баз данных, архитектуры распределенных баз данных, архитектуры клиент/сервер архитектуры и программной среды, элементов разработки хранилищ данных. Модели данных. Реляционная модель данных. Проектирование реляционных баз данных. Этапы проектирования БД. Проектирование данных с помощью модели "сущность-связь". Манипуляционная часть реляционной модели данных. Основы языка SQL. Основные операторы обработки данных в языке SQL.

Результаты изучения:

знать:

- принципы проектирования баз данных;
- нормальные формы;
- методы защиты и безопасности баз данных;

– основы языка SQL;
– архитектуру систем управления реляционными базами данных;
– архитектуру клиент/сервер;

уметь:

– создать реальную реляционную базу данных;
– создавать запросы, представления, процедуры, функции, триггеры на реляционном языке SQL;
– работать в сетевой базе данных;
– работать в сетевой базе данных; умение применять методы защиты и безопасности баз данных;
– применять методы защиты и безопасности баз данных ;
– иметь представления об администрировании баз данных и применять полученные навыки в практической деятельности инженера компьютерной техники.

иметь навыки:

– создания реальных реляционных баз данных на сервере базы данных MSSQLSERVER;
– создания запросов, представлений, процедур, функций, триггеров на реляционном языке T-SQL;
– работы в серверной базе данных MSSQLSERVER;
– применения методов защиты и безопасности серверов баз данных MSSQLSERVER;
– администрирования баз данных MSSQLSERVER и применять полученные навыки в практической деятельности бакалавра компьютерной техники.

Кафедра – Радиотехники и информационной безопасности.

ПРОЕКТИРОВАНИЕ БАЗ ДАННЫХ

Пререквизиты: «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования», «Программирование на языках высокого уровня», «Технологии и методы программирования».

Постреквизиты: «Защита баз данных».

Краткое содержание (основные разделы): Понятие базы данных. Примеры использования и сферы применения баз данных. Методология проектирования баз данных. Этапы и основные принципы проектирования баз данных. Модель "сущность–связь". Реляционная модель данных. Этапы проектирования базы данных и их процедуры. Способы проектирования баз данных. Нормализация таблиц. Ограничения реляционных баз данных. Манипуляционная часть реляционной модели данных. Инструментальные средства проектирования информационных систем. Операторы обработки данных в языке SQL.

Результаты изучения:

знать:

– теоретические основы баз данных, методы обработки данных в базах данных.

– методы и средства проектирования баз данных.
– принципы проектирования реляционных баз данных;
– знать и уметь использовать структурированный язык запросов SQL;
– иметь навыки использования реляционных СУБД для создания баз данных.

уметь:

– уметь разрабатывать концептуальные модели для различных предметных областей;
– разрабатывать и модернизировать программные системы и базы данных;
– использовать метод системного моделирования при исследовании и проектировании программных систем и баз данных;
– уметь использовать структурированный язык запросов SQL;
– использовать методы защиты и безопасности баз данных ;
– администрировать сервера и базы данных.

иметь навыки:

– навыки использования реляционных СУБД для создания баз данных;
– использования баз данных для обработки и интерпретации данных;

– применения методов защиты и безопасности серверов баз данных;
– администрирования баз данных

Кафедра – Радиотехники и информационной безопасности.

БЕЗОПАСНОСТЬ ИНТЕРНЕТ-ТЕХНОЛОГИЙ

Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».

Постреквизиты: «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях», «Защита информации от программных угроз и несанкционированного доступа мобильных устройств».

Цель изучения: формирование у студентов базовых знаний об актуальных угрозах безопасности, о принципах построения и использования современных систем безопасности и защиты Интернет-технологий**.**

Краткое содержание (основные разделы): изучение современных методов, используемых нападающими для проникновения в интернет, принципов действия и возможностей комплексных средств защиты интернет-технологий от несанкционированного доступа. Кроме того дисциплина направлена на углубленное изучение методов и средств обеспечения защиты информации на прикладном и сеансовом уровне, подходов к защите WEB-приложений.

Результаты изучения:

Знать:

- основы организации и функционирования интернет-технологий;
- об основных методах и средствах реализации удаленных сетевых атак на WEB-приложения;
-принципов работы современных средств и методов защиты информации

интернет-технологий;
- основы проектирования и разработки защищенных WEB-приложений.
Уметь:
- определять и устранять основные угрозы интернет-технологий и WEB-приложений;
- выявлять и устранять уязвимости в основных компонентах интернет-технологий;
- проектировать и реализовывать комплексную систему обеспечения защиты интернет-технологий;
- тестировать и на основе результатов тестирования делать обоснованный выбор средств защиты для интернет-технологий и WEB-приложений.
Иметь навыки: позащите от Интернет-атак; о методах и способах защиты информации и данных от копирования.
Кафедра – Радиотехники и информационной безопасности.

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ

Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».
Постреквизиты: «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях», «Защита информации от программных угроз и несанкционированного доступа мобильных устройств».
Цель изучения: формирование у студентов знаний и умений использования средств защиты информации и их практического применения для организации систем защиты современных сетей.
Краткое содержание (основные разделы): изучение общих принципов организации и функционирования современных беспроводных сетей, современных средств анализа и обнаружения информационных атак и методов защиты информации в беспроводных сетях. А также рассматриваются основные протоколы, применяемые для обеспечения безопасности беспроводных сетей.
Результаты изучения:
Знать:
- основы организации и функционирования беспроводной сети;
- основные методы и средства анализа информационных атак беспроводной сети;
- базовые технологии обеспечения защиты и безопасности информации в Беспроводной сети;
- основные практические направления построения систем защиты и безопасности беспроводных сетей.
Уметь:
- использовать в практической деятельности существующие методы и средства контроля и защиты информации в беспроводных сетях;
- применять средства анализа защищенности обнаружения атак в беспроводных сетях;
- организовать практическую защиту информации в беспроводных сетях;

Иметь навыки: по применению технических и программных средств обеспечения безопасности современных беспроводных сетей.
Кафедра – Радиотехники и информационной безопасности.

АДМИНИСТРИРОВАНИЕ ДОМЕННЫХ СИСТЕМ
Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».
Постреквизиты: « Защита баз данных».
Цель изучения: для формирования у студентов основ теоретических знаний и практических навыков по созданию (настройке) доменных систем.
Краткое содержание (основные разделы): технология организации и построения систем, основные компоненты операционных систем и способы взаимодействия компонент, методы и организация доступа в сеть Интернет, принципы администрирования, анализа и управления компонентами защиты операционных систем, основные способы организации безопасной работы в операционной системе, принципы безопасного ввода-вывода информации на различные устройства и организацию потоков и каналов данных, защита и безопасность СУБД.
Результаты изучения:
знать:
– технологию виртуализации серверов Windows (WSV) с широкими возможностями управления и обеспечения безопасности;
– архитектуру и принципы распределенного подхода, требований и критериев построения информационных систем на MS Windows Server;
– принципы администрирования серверов в филиалах на базе службы каталогов Active Directory, включая контроллеры домена;
– физическую модель РБД, локальные вычислительные сети стандарта Ethernet для рабочей группы, топологию и расширение сетей;
– мониторинг и управление сетью, увеличение пропускной способности сети, повышение безопасности сетей;
– принципы работы Windows Server 2008/2012;
уметь:
– развертывать Windows Server 2008/2012, службы каталогов (Active Directory), службы сетевой инфраструктуры (DNS, DHCP, WINS, маршрутизация и удаленный доступ);
– работать с диспетчером серверов, реестром, интерфейсом пользователя;
– работать с командной строкой;
– средствами службы файлов и печати;
– администрировать сетевую OS;
– создавать структуры организационных подразделений (ОП), содержащие учётные записи пользователей и компьютеров;
– управлять учётными записями пользователей и компьютеров;
– создавать группы и управлять ими;
– управлять доступом к сетевым и локальным ресурсам;

– организовывать печать и у управлять печатью;
– управлять доступом к объектам Active Directory с использованием организационных подразделений;
– управлять рабочей средой пользователей и компьютеров с использованием Групповой Политики;
– настраивать аудит учётных записей и ресурсов;
– тестировать политики безопасности компьютера;
– применять полученные навыки в практической деятельности.

иметь навыки:

– диагностики и устранения неисправностей в работе информационных систем;
– работы с приемами защиты информации, обеспечения отказоустойчивости работы серверных систем
– работе с серверным программным обеспечением компании Microsoft.

Кафедра – Радиотехники и информационной безопасности.

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».

Постреквизиты: «Защита баз данных».

Цель изучения: формирование у бакалавров понятий об операционной системе Windows Server 2008/2012, являющейся основой многих корпоративных информационных систем, и имеющей устойчивый спрос на специалистов по администрированию сетей на базе данной операционной системы.

Краткое содержание (основные разделы): изучение теории и получение практических навыков сетевого администрирования информационной системы организации - управления сетевыми узлами, сетевыми протоколами, службами каталогов, сетевыми службами, управления файловыми ресурсами системы, правами доступа к ресурсам, устройствами печати, системами резервного копирования и восстановления информации, осуществления мониторинга сетевых устройств и служб.

Результаты изучения:

знать:

– технологию виртуализации серверов Windows (WSV) с широкими возможностями управления и обеспечения безопасности;
– архитектуру и принципы распределенного подхода, требований и критериев построения информационных систем на MS Windows Server;
– принципы администрирования серверов в филиалах на базе службы каталогов Active Directory, включая контроллеры домена;
– физическую модель РБД, локальные вычислительные сети стандарта Ethernet для рабочей группы, топологию и расширение сетей;
– мониторинг и управление сетью, увеличение пропускной способности сети, повышение безопасности сетей;
– принципы работы Windows Server 2008/2012;

уметь:
- администрировать с помощью удаленного рабочего стола
- управлять учетными записями пользователей
- создавать учетных записей компьютеров
- проводить автоматизацию управления объектами AD DS
- искать объектов в AD DS с помощью запросов
- управлять группами
- создавать организационные единицы
- настраивать делегирования и доверия в Active Directory
- создавать объектов групповой политики.

иметь навыки:
- управления разрешениями для файлов и папок в файловой системе NTFS
- делегирования управления объектами AD DS
- управления областью применения GPO
- настройки политики аудита
- обеспечения доступности серверов и служб
- резервного копирования в Windows Server 2008
- работы с приемами защиты информации, обеспечения отказоустойчивости работы серверных систем.

Кафедра – Радиотехники и информационной безопасности.

№ п/п	Цикл дисциплин	Цифровой код дисциплин	Наименование дисциплины	Семестр	Кол-во кредитов
1	ПД	4306	Оценка рисков и аудит систем информационной безопасности	7	2
		4306	Оценка эффективности корпоративной системы безопасности		
2	ПД	4307	Системы видеонаблюдения и контроля доступа	7	3
		4307	Проектирование систем физической защиты информации		
3	ПД	4308	Моделирование корпоративной комплексной системы защиты информации	7	3
		4308	Проектирование комплексных систем информационной безопасности		

4	ПД	4309	Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях	7	3
		4309	Защита информации от программных угроз и несанкционированного доступа мобильных устройств		
5	ПД	4310	Безопасность и администри-рование систем и сетей	7	3
		4310	Безопасность защищенных вычислительных сетей		
6	ПД	4311	Безопасность баз данных	7	3
		4311	Технологии защиты баз данных		
7	ПД	4223	Защита мобильных устройств	7	2
		4223	Безопасность мобильных систем		

ОЦЕНКА РИСКОВ И АУДИТ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Правовое и информационное обеспечение информационной безопасности», «Безопасность Интернет-технологий», «Программно-аппаратные средства информационной безопасности».

Постреквизиты: итоговая аттестация.

Цель: изучение методов и средств управления информационной безопасностью в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью компании.

Краткое описание: ставит целью ознакомить студентов с проблематикой оценки рисков и аудита систем информационной безопасности; а также развития способностей к логическому и алгоритмическому мышлению, способностей к выяснению сути той или иной проблемы и осуществлению выбора рациональных способов ее преодоления; навыков использования методов исследования и принципов организации систем управления информационной безопасности конкретной компании.

Результаты изучения:

Знать:

-стандарты аудиторской деятельности, этические нормы;

-методику и технологию проведения аудиторской проверки;

-порядок обобщения, оформления и использования результатов аудита;

Уметь:

-составить план, и программу аудиторских проверок системы информационной безопасности;

-применять методы аудита к конкретным объектам проверки;

-оформлять результаты аудиторских процедур;
-сделать выводы по результатам аудита системы информационной безопасности;
Иметь навыки:
- использования методов оценивания информационных рисков;
-применения средств выявления информационных рисков системы;
-владения теоретической базой проведения аудита систем информационной безопасности;
-основных методов проведения аудита к конкретным объектам проверки и оформления результатов ее проведения;
-конкретных практических приемов организации и методологии проведения аудита информационной безопасности в компании;
Кафедра – Радиотехники и информационной безопасности.

ОЦЕНКА ЭФФЕКТИВНОСТИ КОРПОРАТИВНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ

Пререквизиты: «Правовое и информационное обеспечение информационной безопасности», «Безопасность Интернет-технологий», «Программно-аппаратные средства информационной безопасности».
Постреквизиты: итоговая аттестация.
Цель: изучение приобретенных знаний позволят студентам основывать свою профессиональную деятельность на процессном подходе, формировать требования к системе управления информационной безопасности компании, принимать участие в проектировании системы управления информационной безопасности, принимать участие в эксплуатации системы управления информационной безопасности.
Краткое описание: ставит целью ознакомить студентов с навыками использования методов исследования и принципов организации систем управления информационной безопасности конкретной компании.
Результаты изучения:
Знать:
- определение уровней вероятности возникновения рисков и их последствий;
- современные технологии анализа рисков;
- методики идентификации рисков;
- организацию управления рисками, процедуры управления рисками;
- методы принятия решений при обнаружении рисков;
Уметь:
-определить место оценки рисков и аудита систем информационной безопасности в структуре организации и структуре управления информационной безопасностью;
- использовать инструментальные средства при обнаружении рисков и выявлении рисков и принимать решение о выборе защитных средств;
- разрабатывать методы реагирования в случае инцидентов и восстановления работоспособности информационной инфраструктуры компании;
Иметь навыки:

- анализа активов, их угроз информационной безопасности и уязвимостей в рамках области деятельности компании;
- владения методами оценивания информационных рисков;
- использования средств выявления информационных рисков системы;
- построения как отдельных процессов управления информационной безопасности, так и системы процессов в целом.

Кафедра – Радиотехники и информационной безопасности.

СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ И КОНТРОЛЯ ДОСТУПА

Пререквизиты: «Физика», «Информационно-коммуникационные технологии», «Операционная система Linux».

Постреквизиты: итоговая аттестация.

Цель изучения: формирование у студентов основ теоретических знаний и практических навыков к проектированию и эксплуатации систем по физической защиты объектов, ознакомить бакалавров с принципами защиты объектов; способы и средства защиты периметра объектов; способы и средства осуществления охраны объектов на основе систем охранного телевидения; методы и средства контроля эффективности физических средств защиты объектов; способы и средства организации охранно-пожарных сигнализаций и систем пожаротушения; аппаратно-программные средства интеграции физических средств защиты объектов; основы проектирования систем физической защиты объектов..

Краткое содержание (основные разделы): характеристика объектов защиты; способы и средства организации охранно-пожарных сигнализаций и систем пожаротушения; способы и средства защиты периметра объектов; способы и средства осуществления охраны объектов на основе систем охранного телевидения; методы и средства контроля эффективности физических средств защиты объектов; аппаратно-программные средства интеграции физических средств защиты объектов; основы проектирования систем физической защиты объектов.

Знать:

-основные характеристики объектов защиты;

– аппаратно-программные средства интеграции физических средств защиты объектов;

– способы и средства защиты конфиденциальной информации;

– подсистемы комплексной системы охраны объектов;

– основные руководящие документы в области построения охранно-пожарных систем, систем контроля и управления доступом;

– методологии создания систем физической защиты информации;

– основные функции, назначение составных частей и принципы построения систем видеонаблюдения и контроля доступа безопасности;

– назначение отдельных уровней защиты и задачи их работы;

– проблемы построения систем зашиты информации (СЗИ) и организации её функционирования;

– методики проведения сравнительного анализа систем физической защиты информации;
– основные концепции, модели и принципы построения охранных систем и сетей, современные тенденции их развития и стандарты в области видеонаблюдения;
– назначение, принципы построения, эксплуатации и использования систем СКУД;
основы менеджмента современных систем информационной безопасности.
Уметь:
– моделировать объекты защиты;
– выявлять и оценивать угрозы имуществу, жизни и здоровью персонала на конкретных объектах;
– определять рациональные меры защиты на объектах и оценивать их эффективность;
– контролировать эффективность систем физической защиты объектов.
– квалифицированно оценивать область применения элементов видеонаблюдения и СКУД;
– грамотно использовать элементы видеонаблюдения и СКУД при решении практических задач;
– использовать все возможности, предоставляемые системой защиты;
– разрабатывать архитектуру систем видеонаблюдения для заданных требований;
– создавать проект охранной системы, учитывая специфику устройств и руководствуясь принципами функционирования охранных видеокамер и устройств обработки, передачи, приема и фиксации видеоинформации;
– оптимизировать архитектуру системы видеонаблюдения комплексным критериям эффективности, учитывая особенности устройства и принципы функционирования аналоговых, комбинированных и цифровых охранных видеокамер и устройств обработки, передачи, приема и фиксации видеоинформации;
– адекватно управлять системой информационной безопасности, средствами видеонаблюдения и СКУД;
Иметь навыки:
– формальной постановки и решения задач физической защиты объектов;
применения полученных знаний на практике.
Кафедра – Радиотехники и информационной безопасности.

ПРОЕКТИРОВАНИЕ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Пререквизиты: «Физика», «Информационно-коммуникационные технологии», «Операционная система Linux».
Постреквизиты: итоговая аттестация.
Цель изучения: формирование у студентов теоретических знаний и практических навыков к проектированию и эксплуатации систем по физической защиты объектов, ознакомить бакалавров с принципами защиты объектов;

принципов функционирования и техническими возможностями систем видеонаблюдения, способы и средства защиты периметра объектов; методы расчета возможных угроз; способы и средства организации охранно-пожарных сигнализаций и систем пожаротушения; аппаратно-программные средства интеграции физических средств защиты объектов; основы проектирования систем физической защиты объектов.

Краткое содержание (основные разделы): характеристика объектов защиты; способы и средства организации охранно-пожарных сигнализаций и систем пожаротушения; периметровая сигнализация на объекте; системы контроля и управления доступом на объект; аппаратно-программные средства интеграции физических средств защиты объектов; основы проектирования систем физической защиты объектов.

Знать:

-основные характеристики объектов защиты и моделирование угроз;

– аппаратно-программные средства интеграции физических средств защиты объектов;

– методы и средства защиты конфиденциальной информации и объекта;

– подсистемы комплексной системы охраны объектов;

– основные руководящие документы в области построения охранно-пожарных систем, систем контроля и управления доступом;

– методологии создания систем физической защиты информации;

– назначение отдельных уровней защиты и задачи их работы;

– основные функции, назначение составных частей и принципы построения систем видеонаблюдения и контроля доступа безопасности;

– методики проведения сравнительного анализа систем физической защиты объекта

– основные концепции, модели и принципы построения охранных систем и сетей, современные тенденции их развития и стандарты в области видеонаблюдения;

– назначение, принципы построения, эксплуатации и использования систем СКУД;

Уметь:

– моделировать угрозы объекту защиты;

– определять рациональные меры защиты на объектах и оценивать их эффективность; квалифицированно оценивать область применения элементов видеонаблюдения и СКУД;

– грамотно использовать элементы видеонаблюдения, СКУД, Охранно-пожарной и периметровой сигнализации при решении практических задач;

– использовать все возможности, предоставляемые системой защиты;

– разрабатывать архитектуру систем видеонаблюдения для заданных требований;

– создавать проект охранной системы, учитывая специфику устройств и руководствуясь принципами функционирования охранных видеокамер и устройств обработки, передачи, приема и фиксации видеоинформации;

– оптимизировать архитектуру системы видеонаблюдения комплексным критериям эффективности, учитывая особенности устройства и принципы функционирования аналоговых, комбинированных и цифровых охранных видеокамер и устройств обработки, передачи, приема и фиксации видеоинформации;
– адекватно управлять системой информационной безопасности, средствами видеонаблюдения и СКУД и ОПС;

Иметь навыки:

– формальной постановки и решения задач физической защиты объектов;
применения полученных знаний на практике.

Кафедра – Радиотехники и информационной безопасности.

МОДЕЛИРОВАНИЕ КОРПОРАТИВНОЙ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Пререквизиты: «Правовое и информационное обеспечение информационной безопасности», «Безопасность Интернет-технологий», «Программно-аппаратные средства информационной безопасности».

Постреквизиты: итоговая аттестация.

Цель изучения: заложить фундамент комплексного подхода к решению задач информационной безопасности; рассмотреть основные общеметодологические принципы проектирования комплексных систем информационной безопасности; получение студентами знаний о сущности и структуре комплексной системы защиты информации предприятия, об организации защиты информации на предприятии.

Краткое содержание (основные разделы): ставит целью ознакомить студентов с проблематикой моделирования комплексных систем информационной безопасности; а также развития способностей к логическому и алгоритмическому мышлению, способностей к выяснению сути той или иной проблемы.

Результаты изучения:

Знать:

-базовые теоретические понятия лежащие в основе моделирования и анализа комплексного обеспечения информационной безопасности;
-основы и принципы моделирования комплексных систем информационной безопасности;
- общие методологические принципы построения комплексных систем информационной безопасности;

Уметь:

-заложить фундамент комплексного подхода к решению задач информационной безопасности;
-использовать нормативные правовые документы в своей профессиональной деятельности;
-выявлять возможные способы нарушения информационной безопасности при работе систем обработки информации;

-определять виды и формы информации, подверженной угрозам; виды, возможные методы и пути реализации угроз на основе анализа структуры и -- содержания информационных процессов предприятия, целей и задач деятельности предприятия;

Иметь навыки:

-владения методами работы с нормативно-правовыми документами;

-первичной работы с основными средствами обеспечения информационной безопасности;

-оформления рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности;

Кафедра – Радиотехники и информационной безопасности.

ПРОЕКТИРОВАНИЕ КОМПЛЕКСНЫХ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пререквизиты: «Правовое и информационное обеспечение информационной безопасности», «Безопасность Интернет-технологий», «Программно-аппаратные средства информационной безопасности».

Постреквизиты: итоговая аттестация.

Цель изучения: научить применять методы оценки качества систем информационной безопасности; формирование профессиональных компетенций, необходимых для реализации эксплуатационной, проектно-технологической, экспериментально-исследовательской и организационно-управленческой деятельности.

Краткое содержание (основные разделы): ставит целью ознакомить студентов с проблемами и осуществлению выбора рациональных способов её преодоления; навыков использования методов исследования и принципов проектирования комплексных систем информационной безопасности.

Результаты изучения:

Знать:

-комплекс мероприятий по обеспечению информационной безопасности;

-методы и средства проектирования комплексных систем обеспечения информационной безопасности;

Уметь:

-определять задачи комплексной системы информационной безопасности предприятия;

-формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

-оценивать результативность комплексной системы информационной безопасности;

Иметь навыки:

-участия в работах по реализации политики информационной безопасности;

-применения комплексного подхода к обеспечению информационной безопасности в различных сферах деятельности, включая комплекс

организационных мер, учитывающих особенности функционирования предприятия и решаемых им задач.
Кафедра – Радиотехники и информационной безопасности.

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И КАНАЛЫ УТЕЧКИ В ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ

Пререквизиты: «Информационно-коммуникационные технологии», «Математика», «Алгоритмизация и языки программирования», «Организация вычислительных систем и сетей».
Постреквизиты: итоговая аттестация.
Цель изучения: подготовка студентов к эффективному использованию современной компьютерной техники при решении задач и освоение криптографических методов и средств защиты компьютерной информации, изучение методов защиты программ от несанкционированного доступа, построение комплексных систем защиты.
Краткое содержание (основные разделы): классификация систем беспроводной связи, технические концепции построения систем БС, системы с расширением спектра, методы многостанционного доступа, методы разнесения сигналов, основные энергетические параметры систем мобильной связи, новые стандарты защиты беспроводной связи.
Результаты изучения:
Знать:
- роль и место информационной безопасности в системе национальной безопасности государства;
- угрозы информационной безопасности государства;
- современные подходы к построению систем защиты информации;
- компьютерную систему как объект информационного воздействия;

Уметь: - разрабатывать алгоритмы обеспечения безопасности информации и системы;
- знать технологию создания сетевой защиты как данных, так и приложений;

Иметь навыки:
- выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;

Кафедра – Радиотехники и информационной безопасности.

ЗАЩИТА ИНФОРМАЦИИ ОТ ПРОГРАММНЫХ УГРОЗ И НСД МОБИЛЬНЫХ УСТРОЙСТВ

Пререквизиты: «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования», «Системное программирование», «Основы системного программирования», «Программирование на языках высокого уровня», «Скриптовые языки».
Постреквизиты: итоговая аттестация.
Цель изучения: реализация стратегии формирования у студентов практических навыков для качественного и обобщенного использования компьютерных методов вычислительной техники при решении задач и

освоение криптографических методов и средств защиты компьютерной информации, при детальном изучении методов защиты программ от несанкционированного доступа.

Краткое содержание (основные разделы): основные техники и алгоритмы обнаружения НСД, своевременные меры и построение политики безопасного концепта реализации эффективных мер, методы проектирования безопасного периметра, энергетические параметры систем связи, стандарты защиты данных и каналов связи.

Результаты изучения:

Знать:

- ведущее место информационной безопасности в системе безопасности государства;
- возможные угрозы информационной безопасности государства;
- современные подходы к реализации эффектной системы защиты информации;
- классификацию угроз и распределение функционирования системы поэлементно;
- обобщенные критерии оценки защищенности системы и методы обеспечения ее информационной безопасности;
- определенные методики по защите.

уметь:

- эффективно разграничивать ролевую политику и меры, принимаемые в конкретной ситуации;
- прорабатывать технологию создания сетевой защиты данных и приложений в тестовом варианте;
- создавать профильную защиту от несанкционированного доступа к данным.

иметь навыки:

– работы со средствами организации программ по управлению и созданию программ на различных платформах;

– разработчика политики обеспечения безопасности;

– работы со средствами обеспечения целостности и конфиденциальности данных;

– защиты данных криптографическими методами;

- мониторинга и аудита системы доступа к данным;
- выбирать и анализировать показатели качества и критерии оценки систем.

Кафедра – Радиотехники и информационной безопасности.

БЕЗОПАСНОСТЬ И АДМИНИСТРИРОВАНИЕ СИСТЕМ И СЕТЕЙ

Пререквизиты: «Операционная система Linux».

Постреквизиты: итоговая аттестация.

Цель изучения: изучение и формирование знаний студентов в области теоретических основ обеспечение безопасности локальных сетей от атак со стороны интернета, физической и логической структуризации сетей, идеологии открытых систем, многослойной модели сети, конвергенции компьютерных и телекоммуникационных сетей, методов кодирования,

передача трафика через открытые сети путем шифрования передаваемых данных.

Краткое содержание (основные разделы): изучить основы обеспечение безопасности передаваемых данных, технологий передачи данных, методы кодирования и методы доступа к среде передачи.

Результаты изучения:

Знать:

-принципы построения современных вычислительных и систем и сетей, эффективное использование информационных технологий в будущей профессиональной деятельности

- особенности объектов защиты информации, их классификацию, иметь представление о методах и средствах защиты информации при реализации информационных процессов ввода, вывода, передачи, обработкии хранении информации;

Уметь:

- описывать параллельные архитектуры с векторными процессорами (PVP), а также кластерной архитектуры многопроцессорных вычислительных систем (ВС);

- ставить и решать конкретные задачи по применению средств защиты информации для оптимизации функционирования информационных систем (ИС), оценивать уровень безопасности в ИС;

- масштабировать системы, а также совместимость программной среды;

Иметь навыки:

- масштабирования систем, а также совместимость программной среды;

- описания параллельной архитектуры с векторными процессорами (PVP), а также кластерной архитектуры многопроцессорных вычислительных систем (ВС);

- определять необходимые меры защиты информационных ресурсов;

- иметь представления о проектировании аппаратных средств защиты, программных систем защиты, организационных мер защиты.

Кафедра – Радиотехники и информационной безопасности.

БЕЗОПАСНОСТЬ ЗАЩИЩЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Пререквизиты: «Операционная система Linux».

Постреквизиты: итоговая аттестация.

Цель изучения: освоение технологий, принципов организации и функционирования защищенных вычислительных сетей, обучение методам проектирования серверных приложений для использования в среде Интернет.

Краткое содержание (основные разделы): обзор WEB-технологий; знакомство с механизмом работы WEB-серверов; изучение технологии создания серверных WEB-приложений; изучение технологии создания клиентских WEB-приложений; приобретение навыков программирования с помощью скриптового языка PHP; рассмотрение перспектив развития WEB.

Результаты изучения:

уметь: создавать серверные приложения на основе современных WEB-технологий;
знать: принципы технологии для реализации WEB-проектов любого назначения; основы проектирования и защиты информационных систем; системы и модели обработки информации; управлять базами данных; серверный язык программирования PHP;
иметь навыки: проектирования и реализации защищенных WEB-проектов.
Кафедра – Радиотехники и информационной безопасности.

БЕЗОПАСНОСТЬ БАЗ ДАННЫХ
Пререквизиты: «Информационно-коммуникационные технологии», «Алгоритмизация и языки программирования», «Программирование на языках высокого уровня», «Технологии и методы программирования».
Постреквизиты: итоговая аттестация.
Цель изучения: формирование у студентов общих понятий о безопасности баз данных, архитектуры систем безопасности баз данных; понятий реляционной модели, основных элементов стандартного реляционного языка SQL; умение создать защиту реальной базы данных; умение работать в сетевой или локальной базе данных, изучение принципов построения основных моделей данных и их использование в современных системах управления базами данных (СУБД), изучение методов защиты и безопасности баз данных.
Краткое содержание (основные разделы): основные понятия безопасности распределенных баз данных, архитектуры распределенных баз данных, архитектуры клиент/сервер архитектуры и программной среды, элементов разработки хранилищ данных. Модели данных. Реляционная модель данных. Проектирование реляционных баз данных. Этапы проектирования БД. Проектирование данных с помощью модели "сущность-связь". Манипуляционная часть реляционной модели данных. Основы языка SQL. Основные операторы обработки данных в языке SQL.
Результаты изучения:
знать:
– принципы проектирования защищенных баз данных;
– нормальные формы;
– методы защиты и безопасности баз данных;
– основы языка SQL;
– архитектуру систем управления реляционными базами данных;
– архитектуру клиент/сервер;
уметь:
– создать защиту реальной реляционной базы данных;
– создавать запросы, представления, процедуры, функции, триггеры на реляционном языке SQL;
– работать в сетевой базе данных;

– работать в сетевой базе данных; умение применять методы защиты и безопасности баз данных;
– применять методы защиты и безопасности баз данных ;
– иметь представления об администрировании баз данных и применять полученные навыки в практической деятельности инженера компьютерной техники.

иметь навыки:

– создания реальных реляционных баз данных на сервере базы данных MSSQLSERVER;
– создания запросов, представлений, процедур, функций, триггеров на реляционном языке T-SQL;
– работы в серверной базе данных MSSQLSERVER;
– применения методов защиты и безопасности серверов баз данных MSSQLSERVER;
– администрирования баз данных MSSQLSERVER и применять полученные навыки в практической деятельности бакалавра компьютерной техники.

Кафедра – Радиотехники и информационной безопасности.

ТЕХНОЛОГИИ ЗАЩИТЫ БАЗ ДАННЫХ

Пререквизиты: «Информационно-коммуникационные технологии», «Математика», «Алгоритмизация и языки программирования», «Программирование на языках высокого уровня», «Технологии и методы программирования».

Постреквизиты: итоговая аттестация.

Цель изучения: формирование у бакалавров понимания основ информационной безопасности систем баз данных для последующего практического использования. Проблема обеспечения защиты информации является одной из важнейших при построении надежной информационной структуры учреждения на базе ЭВМ. Эта проблема охватывает как физическую защиту данных и системных программ, так и защиту от несанкционированного доступа к данным, передаваемым по линиям связи и находящимся на накопителях, являющегося результатом деятельности как посторонних лиц, так и специальных программ-вирусов. Таким образом, в понятие защиты данных включаются вопросы сохранения целостности данных и управления доступа к данным (санкционированность).

Краткое содержание (основные разделы): Сравнительные исследования серверных СУБД. Основные понятия, концепции и модели структуры распределенных информационных систем. Клиент-серверная архитектура современных реляционных СУБД и АИС. Теоретические основы безопасности БД и СУБД. Методы и механизмы обеспечения целостности информации в реляционных базах данных. Резервное копирование и восстановление баз данных. Распределенные базы данных. Понятия распределенных БД и СУБД. Компонентная архитектура СУРБД. Распределенные транзакции. Репликация данных.

Результаты изучения:
знать:
– основные положения теории баз данных, хранилищ данных, баз знаний;
– основные принципы построения концептуальной, логической и физической
– модели данных;
– современные инструментальные средства разработки схемы базы данных;
– методы описания схем баз данных в современных системах управления базами данных (СУБД);
– структуры данных СУБД, общий подход к организации представлений, таблиц, индексов и кластеров;
– методы организации целостности данных;
– способы контроля доступа к данным и управления привилегиями;
– основные методы и средства защиты данных в базах данных;
– модели и структуры информационных систем;
– основные типы сетевых топологий, приемы работы в компьютерных сетях;
– информационные ресурсы компьютерных сетей;
уметь:
– выделять сущности и связи предметной области;
– отображать предметную область на конкретную модель данных;
пользоваться средствами защиты, предоставляемыми СУБД;
– создавать дополнительные средства защиты;
– проводить анализ и оценку механизмов защиты;
– создавать объекты баз данных в современных системах управления базами данных и управлять доступом к этим объектам;
– работать с современными Case-средствами проектирования баз данных;
формировать и настраивать схему базы данных;
– разрабатывать прикладные программы с использованием языка SQL;
– создавать хранимые процедуры и триггеры на базах данных;
– применять стандартные методы для защиты объектов базы данных.
– основные типы сетевых топологий, приемы работы в компьютерных сетях;
– информационные ресурсы компьютерных сетей;
– технологии передачи и обмена данными в компьютерных сетях;
основы разработки приложений баз данных.
Кафедра – Радиотехники и информационной безопасности.

ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ

Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».
Постреквизиты: «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях», «Защита информации от программных угроз и несанкционированного доступа мобильных устройств».

Цель изучения: формирование у студентов знаний и умений использования мобильных устройств и практического применения для организации систем защиты современных беспроводных сетей.
Краткое содержание (основные разделы): изучение общих принципов организации и функционирования мобильных устройств, современных средств анализа и обнаружения информационных атак и методов защиты информации в мобильной сети. А также рассматриваются основные протоколы, применяемые для обеспечения безопасности беспроводных сетей.
Результаты изучения:
Знать:
- основы организации и функционирования мобильных устройств;
- основные методы и средства защиты мобильных устройств;
- базовые технологии обеспечения защиты и безопасности информации вбеспроводных сетях;
- основные практические направления построения систем защиты и безопасности мобильных сетей.
Уметь:
- использовать в практической деятельности существующие методы и средства контроля и защиты информации в беспроводных сетях;
- применять средства анализа защищенности обнаружения атак в беспроводных сетях;
- организовать практическую защиту информации в беспроводных сетях;
Иметь навыки: по применению мобильных устройст в обеспечении безопасности беспроводных сетей.
Кафедра – Радиотехники и информационной безопасности.

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ СЕТЕЙ

Пререквизиты: «Информационно-коммуникационные технологии», «Операционная система Linux».
Постреквизиты: «Защита от несанкционированного доступа и каналы утечки в инфокоммуникационных сетях», «Защита информации от программных угроз и несанкционированного доступа мобильных устройств».
Цель изучения: формирование у студентов знаний и умений использования средств защиты информации и их практического применения для организации систем защиты современных мобильных сетей.
Краткое содержание (основные разделы): изучение общих принципов организации и функционирования мобильных сетей, современных средств анализа и обнаружения информационных атак и методов защиты информации. А также рассматриваются основные протоколы, применяемые для обеспечения безопасности мобильных сетей.
Результаты изучения:
Знать:
- основы организации и функционирования мобильных сетей;
- основные методы и средства анализа информационных атак;
- базовые технологии обеспечения защиты и безопасности информации в

мобильных сетях;
- основные практические направления построения систем защиты и безопасности мобильных сетей.

Уметь:
- использовать в практической деятельности существующие методы и средства контроля и защиты информации в мобильных сетях;
- применять средства анализа защищенности обнаружения атак в мобильных сетях;
- организовать практическую защиту информации в мобильных сетях;

Иметь навыки: по применению технических и программных средств обеспечения безопасности беспроводных сетей.

Кафедра – Радиотехники и информационной безопасности.