



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования

«Дальневосточный федеральный университет»
(ДВФУ)

Школа естественных наук

УТВЕРЖДАЮ

Директор Школы
естественных наук

Тананаев И.Г.

« 11 » ноября 2019 г.



Сборник
аннотаций рабочих программ дисциплин

СПЕЦИАЛЬНОСТЬ

10.05.01 Компьютерная безопасность

специализация

Математические методы защиты информации

Квалификация выпускника – специалист по защите информации

Форма обучения: *очная*

Нормативный срок освоения программы

(очная форма обучения) *5,5 лет*

Владивосток

2019

Аннотация к рабочей программе дисциплины «Политология»

Рабочая программа учебной дисциплины «Политология» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.8.

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа. Учебным планом предусмотрены лекционные занятия (18 часов), самостоятельная работа студента (54 часа). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – зачет.

Дисциплина логически и содержательно связана с такими курсами, как «Философия», «История», «Основы информационной культуры».

В рамках данного курса изучаются следующие темы: современные политические теории; сущность, источники и механизмы функционирования политической власти; политические режимы; политические партии; государство как основной институт политической системы; международные отношения и мировая политика.

Цель курса - политическая социализация студентов, обеспечение политического аспекта подготовки высококвалифицированных специалистов на основе современной мировой и политической мысли.

Задачи учебного курса:

- дать будущим специалистам первичные политические знания, которые послужат теоретической базой для осмысления социально-политических процессов, для формирования политической культуры, выработки личной позиции и более четкого понимания меры своей ответственности,
- развить навыки самостоятельной оценки информации политического характера.

Для успешного изучения дисциплины «Политология» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);
- способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);
- способность к самоорганизации и самообразованию (ОК-8);
- способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований (ПК-2).

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
(ОК-5) способность понимать социальную значимость своей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Знает	о месте и роли своей будущей профессии для общества и государства.
	Умеет	применить полученные навыки в области политологии в профессиональной деятельности в условиях информационного противоборства.
	Владеет	пониманием связи своей профессиональной деятельности с безопасностью личности, общества и государства.

Для формирования вышеуказанных компетенций в рамках дисциплины «Политология» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), конспект (ПР-7), реферат (ПР-4).

Аннотация к рабочей программе дисциплины «Основы управленческой деятельности»

Рабочая программа учебной дисциплины «Основы управленческой деятельности» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.11.

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 академических часа. Учебным планом предусмотрены лекционные занятия (18 часов), практические занятия (18 часов) и самостоятельная работа студента (36 часов). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – зачёт.

Дисциплина логически и содержательно связана с такими курсами, как «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

Изучение дисциплины направлено на развитие комплексного представления о системе менеджмента, его элементах, процессах и механизмах. Рассмотрены этапы развития менеджмента, цели, функции и методы управления фирмой, процесс принятия решений, организационные структуры управления, человеческий фактор в менеджменте, типы руководителей, управленческие конфликты.

Цель – формирование у студентов представлений об утвердившемся в экономике России принципиально новом подходе к собственности и сформировавшемся равноправии ее форм, что на практике означает экономическую свободу для инициативной хозяйственной деятельности организационно-правовых структур любой формы собственности в рамках действующего законодательства.

Задачи – дать студентам базовые знания о:

- предприятиях (организациях) различных форм собственности, включая существующие организационно-правовые формы, в которых может осуществляться их деятельность;
- необходимые для их создания и функционирования нормативно-правовые документы;
- принципы организации производства и управления в них.

Для успешного изучения дисциплины «Основы управленческой деятельности» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5)
- способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9)
- способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем (ПК-16)

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные и профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ОК-6) способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Знает	принципы эффективной работы в коллективе.
	Умеет	эффективно разрешать возникающие конфликты; толерантно воспринимать социальные, культурные и иные различия.
	Владеет	опытом работы в коллективе.

(ПК-13) способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности	Знает	способы организации работы в малых коллективах исполнителей.
	Умеет	находить и принимать управленческие решения в сфере профессиональной деятельности.
	Владеет	опытом работы с малым коллективом исполнителей.

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы управленческой деятельности» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Теория вероятностей и математическая статистика»

Рабочая программа учебной дисциплины «Теория вероятностей и математическая статистика» разработана для студентов, обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.14.

Дисциплины составляет 7 зачетных единиц, 252 академических часа. Учебным планом предусмотрены лекции (72 часа), практические занятия (54 часа), самостоятельная работа студента (126 часов, в том числе 36 часов на подготовку к экзамену). Дисциплина реализуется на 3 курсе в 5 и 6 семестрах. Форма контроля по дисциплине: в 5,6 семестрах зачет, в 6 семестре экзамен.

Курс «Теория вероятностей и математическая статистика» непосредственно связан с дисциплинами «Алгебра», «Математический анализ», «Численные методы и математическое моделирование».

По завершению обучения по дисциплине студент должен овладеть знаниями основ теории вероятности; иметь представление о роли и месте теории вероятности в математических науках в целом, о роли теории вероятности в физике; уметь использовать законы теории вероятности для решения задач.

Цель курса - ознакомить студентов с основами теории вероятности, а также с методами решения вероятностных задач в физике и других областях приложения теории вероятности.

Задачи:

- изучение общих принципов описания стохастических явлений;
- ознакомление студентов с вероятностными методами исследования прикладных вопросов;
- формирование навыков самостоятельного изучения специальной литературы, понятия о разработке математических моделей для решения практических задач;

- развитие логического мышления, навыков математического исследования явлений и процессов, связанных с профессиональной деятельностью.

- формирование представления о месте и роли теории вероятностей и математической статистики в современном мире;

- формирование системы основных понятий, используемых для описания важнейших вероятностных моделей и методов, и раскрытие взаимосвязи этих понятий.

Для успешного изучения дисциплины «Теория вероятностей и математическая статистика» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения (ОПК-7);
- способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПК-4);
- способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем (ПК-7).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-2 - способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической	Знает	необходимые математические законы и методы решения задач.
	Умеет	использовать средства вычислительной техники для решения профессиональных задач.
	Владеет	опытом решения профессиональных задач с

логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	применением математического аппарата.
--------------------------------------------------------------------------------------------------------------------------	---------------------------------------

Для формирования вышеуказанных компетенций в рамках дисциплины «Теория вероятностей и математическая статистика» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Языки программирования»

Курс учебной дисциплины «Языки программирования» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.21.

Общая трудоемкость дисциплины составляет 252 часа (7 з.е.). Учебным планом предусмотрены лекции – 36 часов, практические занятия – 8 часов, лабораторные работы – 64 часа, самостоятельная работа – 144 часов, в том числе 36 часов на подготовку к экзамену. Дисциплина реализуется на 4 курсе в 7 и 8 семестре. Форма контроля по дисциплине – в 7 семестре экзамен, в 8 семестре зачет.

Дисциплина «Языки программирования» базируется на предварительном изучении следующих дисциплин: «Информатика», «Дискретная математика».

Содержание дисциплины охватывает следующий круг вопросов: основные структуры и инструментарий, которые применяются в языках программирования, основные структуры и типы данных, основные методы при разработке алгоритмов (рекурсия, отход назад, метод ветвей и границ, анализ арифметических выражений), базовые алгоритмы на динамических структурах данных, библиотеки стандартных программ.

Цель изучения дисциплины «Языки программирования» заключается в ознакомлении студентов с основами технологии проектирования сложных программных комплексов, основами объектно-ориентированных языков программирования, алгоритмами, методами и способами построения сложных программ, изучении языка программирования C++, выработке навыков проектирования программных комплексов и программирования.

Задачи:

- знакомство студентов с основными видами языков программирования

высокого уровня;

- формирование навыков работы с различными средствами программирования и отладки для создания программного обеспечения на языках высокого уровня;

- обучение основным принципам алгоритмического подхода от этапа формализации до реализации в виде программного кода.

Для успешного изучения дисциплины «Языки программирования» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-4 – способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными	Знает	основные приемы разработки объектно-ориентированных программ на языках высокого уровня; перечень программного обеспечения, которое может быть использовано в процессе разработки объектно-ориентированных программ
	Умеет	работать с программными средствами прикладного, системного и специального назначения для разработки объектно-ориентированных программ

проектами	Владеет	навыками самостоятельно работать с различными средствами программирования и отладки для создания программного обеспечения на языках высокого уровня
ОПК-8 – способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Знает	перечень программного обеспечения интегрированной среды разработки для реализации объектно-ориентированных программ
	Умеет	разрабатывать объектно-ориентированные программы (подпрограммы) на языках программирования высокого уровня
	Владеет	навыками работы с различными средствами программирования и отладки для создания программного обеспечения на языках высокого уровня для решения физических задач

Для формирования вышеуказанных компетенций в рамках дисциплины «Языки программирования» применяются следующие методы обучения: чтение лекций, проведение и сдача лабораторных работ в интегрированной среде разработки Microsoft Visual Studio. Используемые оценочные средства: собеседование (ОУ-1), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Операционные системы и оболочки»

Курс учебной дисциплины «Операционные системы и оболочки» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовой дисциплины учебного плана Б1.Б.22.1.

Общая трудоемкость дисциплины составляет 144 часа (4 з.е.). Учебным планом предусмотрены лекционные занятия (18 часов), практические занятия (18 часов), самостоятельная работа студента (72 часа), подготовка к экзамену (36 час.). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Операционные системы и оболочки» логически и содержательно связана с такими курсами, как «Языки программирования», «Системы управления базами данных», «Методы программирования».

Содержание дисциплины охватывает следующий круг вопросов: общая характеристика операционных систем, типы адресации памяти в микропроцессорах фирмы intel, многозадачный режим, алгоритмы планирования, синхронизация потоков, механизмы прерываний в ОС, общая характеристика файловой системы.

Цель изучения дисциплины «Операционные системы и оболочки» заключается в ознакомлении студентов с современными операционными системами, классификацией, архитектурой их построения, а также с сетевыми компонентами многозадачных операционных систем.

Задачи:

- дать студенту теоретические и практические знания по построению и эксплуатации операционных систем ЭВМ;
- знание основ функционирования и структуры современных операционных систем;
- способность использовать средства операционных систем в разработке и эксплуатации информационных систем;

- формирование профессиональных компетенций в области разработки информационных систем в соответствии с требованиями ФГОС ВО по данному направлению подготовки.

Для успешного изучения дисциплины «Операционные системы и оболочки» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8);

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

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

В результате изучения данной дисциплины у студентов формируются следующие общепрофессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-3) способность понимать значение информации в развитии современного общества, применять достижения информационных	Знает	правила эксплуатации средств вычислительной техники.
	Умеет	использовать современную вычислительную технику и программное обеспечение для проведения организационно-управленческих расчетов.

технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	Владеет	работы на персональном компьютере под управлением конкретной операционной системы и разработки приложений с использованием офисных программных средств.
(ОПК-4) способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знает	правила эксплуатации средств вычислительной техники.
	Умеет	использовать современную вычислительную технику и программное обеспечение для проведения организационно-управленческих расчетов.
	Владеет	работы на персональном компьютере под управлением конкретной операционной системы и разработки приложений с использованием офисных программных средств.

Для формирования вышеуказанных компетенций в рамках дисциплины «Операционные системы и оболочки» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Операционная система UNIX»

Рабочая программа «Операционная система UNIX» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в базовую часть учебного плана Б1.Б.22.2.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 академических часов. Учебным планом предусмотрены лекционные занятия (18 часов), лабораторные работы (18 часов), самостоятельная работа (72 час.) Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Операционная система UNIX» логически и содержательно связана с такими курсами, как «Информатика», «Методы программирования».

Содержание дисциплины охватывает следующий круг вопросов: состав и основные свойства интеллектуальных информационных систем; модели и методы представления знаний; инструментальные средства разработки систем искусственного интеллекта; основные метапроцедуры и стратегии управления базами знаний; методы извлечения, приобретения и формирования знаний; принципы и методы структурирования и формализации знаний; онтологии; мультиагентные системы и технологий.

Цель: познакомить студентов с семейством UNIX-подобных систем, которые используются как на серверах, так и рабочих станциях там, где необходима высокая производительность компьютера (базы данных, работа с графикой, роутеры и т.д.).

Задачи:

- дать студенту теоретические и практические знания по построению и эксплуатации операционных систем ЭВМ;
- приобрести основные понятия об ОС UNIX; о полномочиях и доступе к ресурсам ОС; о маршрутизации и администрирование TCP/IP сети.

Для успешного изучения дисциплины «Операционная система UNIX» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-3 - способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	Знает	основные понятия информатики; назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных.
	Умеет	использовать программные и аппаратные средства персонального компьютера.
	Владеет	навыками поиска информации в глобальной информационной сети интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, субд и т.п.).
ОПК-4 - способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарным и инновационными проектами	Знает	методы научных исследований, основные понятия, категории и инструменты анализа проекта.
	Умеет	использовать интернет-ресурсы, полнотекстовые баз данных и каталогов, электронные журналы и патенты, поисковые ресурсы для поиска информации
	Владеет	основными приемами анализа, технологии выполнения наиболее типичных операций применительно к сфере своей деятельности

Для формирования вышеуказанных компетенций в рамках дисциплины «Операционная система UNIX» применяются следующие методы активного/

интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Windows – операционные системы»

Курс учебной дисциплины «Windows – операционные системы» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.22.3.

Общая трудоемкость освоения дисциплины составляет 108 часов (3 з.е.). Учебным планом предусмотрены, лабораторные работы (32 час.), практические занятия (4 часа), самостоятельная работа студента (72 час.). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Windows – операционные системы» логически и содержательно связана с такими курсами, как «Информатика», «Операционные системы и оболочки», «Методы программирования».

Содержание дисциплины охватывает следующий круг вопросов: обучение работе с операционными системами Windows на уровне, который позволяет устанавливать, настраивать, обслуживать и обеспечивать безопасное функционирование операционных систем.

Цель изучения дисциплины «Windows – операционные системы» заключается в формировании у студентов компетенций в области администрирования операционных систем Windows.

Задачи:

- дать основы назначения, принципов построения, эксплуатации и использования операционных систем Windows;
- сформировать практические навыки установки, настройки и администрирования операционных систем Windows;
- обучить основным настройкам сетевых параметров операционных систем Windows;

- обучить особенностям настройки систем безопасности операционных систем Windows.

Для успешного изучения дисциплины «Windows – операционные системы» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-3 – способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	Знает	историю развития операционных систем; требования к операционным системам; основные принципы функционирования операционных систем
	Умеет	осуществлять целенаправленный поиск по научно-технической информации по заданной теме; администрировать операционные системы на базовом уровне; разрабатывать простые приложения для распространенных операционных систем, используя стандартные инструменты разработчика и библиотеки программных компонентов
	Владеет	навыками самостоятельной научно-исследовательской работы
ОПК-4 – способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знает	параметры загрузки операционной системы; выполнение конфигурирования аппаратных устройств; управление учетными записями, настройку параметров рабочей среды пользователей; управление дисками и файловыми системами, настройку сетевых параметров, управление разделением ресурсов в локальной сети; создание и выполнение командных файлов в семействах "Windows"
	Умеет	устанавливать операционные системы семейств "Windows"; компилировать программы в семействах

	"Windows"; создавать процессы и использовать системные вызовы
Владеет	навыками самостоятельной разработки и написания программ, согласно методам проектирования программного обеспечения

Для формирования вышеуказанных компетенций в рамках дисциплины «Windows – операционные системы» применяются следующие методы активного/интерактивного обучения: работа в малых группах, метод обучения в парах, проведение и сдача лабораторных работ, собеседование по итогам выполнения практических заданий. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6).

Аннотация к рабочей программе дисциплины «Системы управления базами данных»

Курс учебной дисциплины «Системы управления базами данных» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.23.

Общая трудоемкость дисциплины составляет 252 часа (7 з.е.). Учебным планом предусмотрены лекции – 36 часов, лабораторная работы – 56 часов, практические занятия – 34 часа, самостоятельная работа – 90 часов, подготовка к экзамену – 36 часов. Дисциплина реализуется на 3 курсе в 5 и 6 семестрах. Форма контроля по дисциплине – в 5 семестре зачет, в 6 семестре экзамен.

Дисциплина «Системы управления базами данных» логически и содержательно связана с таким курсом, как «Информатика», «Методы программирования».

Содержание дисциплины охватывает следующий круг вопросов: смысл и методы абстрагирования данных, характеристики и типы систем баз данных, области применения систем управления базами данных, этапы проектирования баз данных, физическую организацию баз данных, средства поддержания целостности в базах данных, особенности управления данными в системах распределенной обработки, порядок эксплуатации баз данных.

Цель изучения дисциплины «Системы управления базами данных» заключается в освоении принципов хранения, обработки и передачи информации в автоматизированных системах, методов проектирования баз данных и реализации прикладного программного обеспечения на базе современных систем управления базами данных (СУБД).

Задачи:

- знакомство с моделями данных, используемыми в СУБД, основой теории реляционных баз данных и методами проектирования баз данных;

- приобретение навыков практического использования методов проектирования баз данных реляционного типа;
- подробное изучение конкретной СУБД реляционного типа, ее возможностей и особенностей;
- приобретение навыков реализации прикладного программного обеспечения с помощью выбранной СУБД.

Для успешного изучения дисциплины «Системы управления базами данных» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);
- способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8).

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные, общепрофессиональные и профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-4 – способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знает	смысл и методы абстрагирования данных.
	Умеет	формировать цель создания системы управления базами данных; принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность
	Владеет	навыками создания систем управления базами данных
ПК-5 – способность участвовать в разработке и	Знает	основные модели данных, используемых в СУБД, основу теории реляционных баз

конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		данных и методы проектирования баз данных
	Умеет	готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ
	Владеет	знаниями по последним обновлениям баз данных
ПК-10 – способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает	перечень программного обеспечения интегрированной среды разработки для настройки эффективной работы базы данных
	Умеет	учитывать особенности работы в базе данных, пользоваться инструментальными средствами конкретной базы данных
	Владеет	навыками работы с различными средствами программирования; навыками отладки программного обеспечения

Для формирования вышеуказанных компетенций в рамках дисциплины «Системы управления базами данных» применяются следующие методы активного/интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах, чтение лекций с использованием мультимедийного оборудования (проектор), проведение и сдача лабораторных работ, собеседование по итогам выполнения практических заданий. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Электроника и схемотехника»

Курс учебной дисциплины «Электроника и схемотехника» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.24.

Общая трудоемкость дисциплины составляет 216 часов (6 з.е.). Учебным планом предусмотрены лекции (36 час.), практические занятия (4 часа), лабораторные работы (50 час.), самостоятельная работа студента (81 час). Дисциплина реализуется на 3 курсе в 6 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Электроника и схемотехника» логически и содержательно связана с таким курсом, как «Физические основы механики», «Электричество и магнетизм».

Содержание дисциплины охватывает следующий круг вопросов: изучение основных принципов работы генераторов, усилителей; схемы электрических цепей, схемы замещения реальных элементов и источников, основные понятия топологии цепей, логические функции и логические элементы.

Цель курса – формирование системы знаний, позволяющих применять в практической деятельности радиоэлектронные методы измерений, постановки и организации экспериментов, автоматизации получения, накопления и обработки экспериментальных данных; привитие навыков и умений работать со специальной аппаратурой по радиоэлектронике.

Задачами дисциплины являются:

- формирование специальных физических, математических, теоретических и практических знаний, которые обеспечили бы возможность понимать и анализировать процессы в радиоэлектронных цепях систем обработки информации;

- привитие навыков в использовании методов анализа базовых элементов и микросистемных устройств, применяемых в системах передачи и обработки информации;
- приобретение опыта использования элементной базы радиоэлектронной аппаратуры;
- формирование способности к самостоятельному и инициативному решению технических проблем;
- обучение основам элементной базы полупроводниковой электроники, схемотехники электронных аналоговых устройств, схемотехники электронных цифровых устройств, схемотехники смешанных аналогово-цифровых устройств, устройств отображения информации.

Для успешного изучения дисциплины «Электроника и схемотехника» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность анализировать физические явления и процессы при решении профессиональных задач (ОПК-1).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций).

Код и формулировка компетентности	Этапы формирования компетентности	
ОПК-3 – способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	Знает	принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них; основы схемотехники современной радиоэлектронной аппаратуры
	Умеет	проводить расчеты типовых аналоговых и цифровых узлов радиоэлектронной аппаратуры
	Владеет	навыками анализа; навыками технологии выполнения наиболее типичных операций применительно к сфере своей деятельности

Для формирования вышеуказанных компетенций в рамках дисциплины «Электроника и схемотехника» применяются следующие методы активного/интерактивного обучения: интерактивные и проблемные лекции, лекции-

диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Техническая защита информации»

Курс учебной дисциплины «Техническая защита информации» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.26.

Общая трудоемкость освоения дисциплины составляет 108 часа (3 з.е.). Учебным планом предусмотрены лекционные занятия (36 час), лабораторные работы (16 час), практические занятия (2 час.), самостоятельная работа (54 час). Дисциплина реализуется на 5 курсе, в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Техническая защита информации» логически и содержательно связана с такими курсами, как "Цифровая электроника" и "Операционные системы".

Содержание дисциплины охватывает следующий круг вопросов: технические каналы утечки информации и средства технической защиты информации.

Цель дисциплины: выработать умения и навыки по определению потенциальных каналов утечки информации на объектах информатизации, по выработке рекомендаций по защите конкретного канала утечки, ознакомить с процессом сертификации средств защиты и мероприятиями аттестации объектов информатизации на соответствие требованиям безопасности информации.

Задачи дисциплины:

- раскрыть природу формирования технических каналов утечки информации;
- сформировать представление о проблемах защиты технических каналов утечки информации;
- достижение указанных целей включает последовательное изложение материала, с указанием причинно-следственных связей, отработку приемов

решения поставленных задач на практических занятиях.

Для успешного изучения дисциплины «Техническая защита информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);
- способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-18).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-9) способность разрабатывать формальные модели политик безопасности, политик управления доступом и	Знать	основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды

информационными потоками компьютерных системах с учетом угроз безопасности информации	В	и безопасности информационных потоков
	Уметь	разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
	Владеть	навыками разработки моделей угроз и моделей нарушителя
(ПК-19) способность производить проверку технического состояния и профилактические осмотры оборудования по защите информации	Знать	принципы работы оборудования по защите информации
	Уметь	проводить проверку технического состояния оборудования по защите информации
	Владеть	навыками настройки оборудования по защите информации

Для формирования вышеуказанных компетенций в рамках дисциплины «Техническая защита информации» применяются следующие методы активного/ интерактивного обучения: дискуссия и презентация. Используемые оценочные средства: коллоквиум (ОУ-2), реферат (ПР-4), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Модели безопасности компьютерных систем»

Курс учебной дисциплины «Модели безопасности компьютерных систем» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.27.

Общая трудоемкость освоения дисциплины составляет 108 часов (3 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), практические занятия (32 час.), лабораторные работы (4 час.), самостоятельная работа студентов (68 час.). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Модели безопасности компьютерных систем» логически и содержательно связана с такими курсами, как: «Информатика», «Математическая логика и теория алгоритмов», «Дискретная математика», «Основы информационной безопасности».

Содержание дисциплины охватывает следующий круг вопросов: классификация современных компьютерных систем, основные понятия математической логики и теории алгоритмов, источники и классификация угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, защитные механизмы и средства обеспечения безопасности операционных систем.

Цель курса – обучение специалистов принципам построения формальных моделей политик безопасности, политик управления доступом и информационными потоками, методам анализа математических моделей защищаемых систем и систем обеспечения информационной безопасности КС.

Задачи:

- изучение основных угроз безопасности информации и модели нарушителя в КС.
- изучить основные виды политик управления доступом и информационными потоками в КС.
- изучить основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
- научить разрабатывать модели угроз и модели нарушителя безопасности КС.
- научить разрабатывать частные политики безопасности КС, в том числе политики управления доступом и информационными потоками.

Для успешного изучения дисциплины «Модели безопасности компьютерных систем» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

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

- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);

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

В результате изучения дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-7) способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах. основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Умеет	осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем.
	Владеет	навыком формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем
(ОПК-9) способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах. основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Умеет	использовать основные виды политик управления доступом и информационными потоками в компьютерных системах. использовать основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Владеет	методами разработки частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками.
(ПК-4) способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знает	математические основы моделей безопасности. основы постановки научной задачи, определения гипотезы и методов исследования безопасности компьютерных систем

	Умеет	построить формальную модель системы, соответствующую заданной политике безопасности. научно и теоретически обосновано излагать результаты исследований безопасности компьютерных систем
	Владеет	методами анализа безопасности компьютерных систем с использованием формальных моделей безопасности. методиками исследований в области безопасности компьютерных систем

Для формирования вышеуказанных компетенций в рамках дисциплины «Модели безопасности компьютерных систем» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, работа в малых группах, выполнение практических работ. Используемые оценочные средства: коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Криптографические методы защиты информации»

Курс учебной дисциплины «Криптографические методы защиты информации» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.28.

Общая трудоемкость освоения дисциплины составляет 216 часов (6 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (18 час.), практические занятия (90 час.), самостоятельная работа студентов (72 час.). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Криптографические методы защиты информации» логически и содержательно связана с такими курсами, как «Математический анализ», «Основы геометрии», «Алгебра».

Содержание дисциплины охватывает следующий круг вопросов: комплексные числа, множества на комплексной плоскости, основные элементарные функции комплексного переменного, многозначные функции. Дисциплина направлена на формирование общекультурных, общепрофессиональных и профессиональных компетенций выпускника.

Цель дисциплины - изложить основополагающие принципы защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины:

- дать основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;

- изучить принципов синтеза и анализа шифров;

- ознакомить с математическими методами, используемых в криптоанализе.

Для успешного изучения дисциплины «Криптографические методы защиты информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-4) способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знает	методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.
	Умеет	применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.
	Владеет	методикой и методологией научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.
(ОПК-10) способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Знает	современные языки программирования и программные комплексы.
	Умеет	строить алгоритмы.
	Владеет	навыком самостоятельного построения алгоритма, проведения его анализа и реализацией в современных программных комплексах.

Для формирования вышеуказанных компетенций в рамках дисциплины «Криптографические методы защиты информации» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, работа в малых группах, выполнение практических работ. Используемые оценочные средства: коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Криптографические протоколы»

Курс учебной дисциплины «Криптографические протоколы» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.29.

Общая трудоемкость освоения дисциплины составляет 252 часа (7 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), практические занятия (90 час.), самостоятельная работа (126 час.). Дисциплина реализуется на 3 курсе в 6 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Криптографические протоколы» логически и содержательно связана с такими курсами, как «Математическая логика и теория алгоритмов», «Дискретная математика», «Криптографические методы защиты информации».

Содержание дисциплины охватывает следующий круг вопросов: основные понятия компьютерных технологий и теории криптографических протоколов. Дисциплина направлена на формирование общекультурных, общепрофессиональных и профессиональных компетенций выпускника.

Цель дисциплины – сформировать представление об использовании криптографических протоколов для защиты информации, о принципах применения совершенных информационных технологий.

Задачи дисциплины:

- дать основы знаний об основных криптографических протоколах;
- познакомить с методикой выбора и оценки их качества.

Для успешного изучения дисциплины «Криптографические протоколы» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над

междисциплинарными и инновационными проектами (ОПК-4);

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	Код и формулировка компетенции
ОПК-2 - способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Знает	необходимые математические законы и методы решения задач;
	Умеет	использовать средства вычислительной техники для решения профессиональных задач;
	Владеет	опытом решения профессиональных задач с применением математического аппарата
ОПК-9 - способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	базовые протоколы проверки подлинности и обмена ключами. основные криптологические аспекты проектирования и развертывания технологии ркi в корпоративных сетях (стандарт х.509). протоколы обеспечения безопасности в сети internet. основные подходы к конструированию систем защиты информации с использованием криптографических протоколов различной направленности.
	Умеет	проектировать и внедрять схемы аутентификации на основе типовых стандартизированных механизмов. использовать схемы разделения секрета для хранения критической информации. осуществлять распределение

		аутентифицированных криптографических ключей в корпоративных сетях анализировать защищенность системы, использующей криптографические протоколы, в модели уязвимой среды долева-яо квалифицированно оценивать информационные риски, возникающие при использовании конкретных криптографических протоколов в защищаемой информационной системе.
	Владеет	навыком настройки параметров протоколов используемых для аутентификации и обмена ключами в операционных системах семейства windows. навыком генерирования ключевых пар с использованием пакета open-ssh. навыком использования и администрирования современных средств электронной цифровой подписи. навыком самостоятельной работы с современными международными стандартами криптографических протоколов.

Для формирования вышеуказанных компетенций в рамках дисциплины «Криптографические протоколы» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, работа в малых группах, выполнение практических работ. Используемые оценочные средства: коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Цифровая электроника»

Курс учебной дисциплины «Цифровая электроника» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.30.1.

Общая трудоемкость освоения дисциплины составляет 144 часов (4 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (32 час.), практические занятия (4 час.) самостоятельная работа студента (72 час.). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Цифровая электроника» логически и содержательно связана с такими курсами, как «Сети ЭВМ и телекоммуникации», «Схемотехника телекоммуникационных устройств», «Общая теория связи»,

Содержание дисциплины охватывает следующий круг вопросов: основы цифровой схемотехники, принципы работы и проектирования цифровых устройств, основные методы описания и синтеза логических схем, современные средства разработки цифровых устройств. Дисциплина направлена на формирование общекультурных, общепрофессиональных и профессиональных компетенций выпускника.

Цель освоения дисциплины «Цифровая электроника» является формирование устойчивых знаний, умений и владений в области разработки и применения цифровых электронных элементов.

Задачи:

- сообщить студентам основной комплекс знаний, необходимых для понимания физически;
- обоснованных принципов реализации логических элементов;
- привить навыки практического использования алгебры логики и базовых логических;
- элементов для построения цифровых устройств.

Для успешного изучения дисциплины «Цифровая электроника» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-4) способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знает	перспективные технологии и стандарты
	Умеет	содействовать внедрению перспективных технологий и стандартов
	Владеет	методами внедрения перспективных технологий и стандартов связи
(ПК-18) способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах. основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Умеет	использовать основные виды политик управления доступом и информационными потоками в компьютерных системах. использовать основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Владеет	методами разработки частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками.

Для формирования вышеуказанных компетенций в рамках дисциплины «Цифровая электроника» применяются следующие методы активного/интерактивного обучения: имитационные модели, интерактивные и проблемные лекции. Используемые оценочные средства: коллоквиум (ОУ-2), лабораторные работы (ПР-6).

Аннотация к рабочей программе дисциплины «Микропроцессоры»

Рабочая программа учебной дисциплины «Микропроцессоры» разработана для студентов, обучающихся по специальности 10.05.01 «Компьютерная безопасность», профиль «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.30.2.

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 144 академических часа. Учебным планом предусмотрены лекции (36 час.), лабораторные работы (32 час.), практические занятия (4 час.), самостоятельная работа студента (72 час.). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – экзамен, зачет.

Дисциплина связана с предшествующими дисциплинами: Цифровая электроника, Электроника и схемотехника, Аппаратные средства вычислительной техники и Архитектура персонального компьютера.

В курсе лекций дисциплины «Микропроцессоры» основное внимание уделяется общетеоретическим положениям анализа и проектирования достаточно простых цифровых устройств комбинационного и последовательностного типов (логических элементов, мультиплексоров, триггеров, регистров, счетчиков и др.), являющихся базой для построения сложных БИС микропроцессоров и микропроцессорного обрамления, а также принципам построения и функционирования микропроцессоров и радиотехнических устройств на их основе. В первых разделах рассматриваются преимущества цифровых устройств, перечислены области их оптимального применения, приводятся классификация и определения устройств различных типов, материал иллюстрируется примерами реального использования. Далее приводятся характеристики микропроцессоров различных поколений их системы команд, особенности программирования и аппаратное устройство микропроцессорных устройств и систем (контроллеры, порты и т.д.).

Целью курса является: изучение методов синтеза цифровых устройств и методов проектирования микропроцессорных устройств, а также формирование практических навыков проектирования цифровых и микропроцессорных систем

Задачи:

- формирование у студентов соответствующего уровня знаний, достаточного для исследования реализации командного цикла процессора на уровне микроопераций;
- изучения способов организации взаимодействия процессора и внешних устройств в составе ЭВМ.

Для успешного изучения дисциплины «Микропроцессоры» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-4) способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знает	перспективные технологии и стандарты
	Умеет	содействовать внедрению перспективных технологий и стандартов
	Владеет	методами внедрения перспективных технологий и стандартов связи

(ПК-18) способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах. основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Умеет	использовать основные виды политик управления доступом и информационными потоками в компьютерных системах. использовать основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Владеет	методами разработки частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками.

Для формирования вышеуказанных компетенций в рамках дисциплины «Микропроцессоры» применяются следующие методы активного/интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ЛР-6), конспект (ЛР-7).

Аннотация к рабочей программе дисциплины «Архитектура персонального компьютера»

Рабочая программа учебной дисциплины разработана для студентов, обучающихся по специальности 10.05.01 «Компьютерная безопасность», профиль «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.30.3.

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 академических часа. Учебным планом предусмотрены лекции (30 час.), лабораторные занятия (2 час.), практические занятия (4 час.), самостоятельная работа студента (36 час.). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Архитектура персонального компьютера» логически и содержательно связана с такими курсами, как «Электроника и схемотехника», «Цифровая электроника».

Содержание дисциплины охватывает следующий круг вопросов: функциональная и структурная организация ЭВМ и систем, информационно-логические основы ЭВМ, многопрограммные вычислительные системы.

Цель курса - изучение теоретических основ и принципов построения вычислительных машин и систем, их функциональной и структурной организации, характеристик основных устройств персональных ЭВМ (ПЭВМ) и вычислительных систем, режимов работы ЭВМ и систем, организации вычислительного процесса, взаимодействия аппаратных и программных средств.

Задачи курса – сформировать у студента навыки и умения:

- оценивать технико-эксплуатационные возможности ЭВМ и вычислительных систем;
- знать принципы построения, состав, назначение аппаратного и программного комплексов ЭВМ, особенности их функционирования и реализации различных режимов работы вычислительных систем;

- знать характеристики основных устройств персональных ЭВМ и вычислительных систем;

- разбирать и собирать персональный компьютер, проводить установку и настройку операционного и прикладного программного обеспечения;

- практические навыки эффективного использования аппаратных и программных средств ЭВМ при решении экономических и других задач.

Для успешного изучения дисциплины «Микропроцессоры» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-4) способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знает	перспективные технологии и стандарты
	Умеет	содействовать внедрению перспективных технологий и стандартов
	Владеет	методами внедрения перспективных технологий и стандартов связи
(ПК-18) способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков

информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Умеет	использовать основные виды политик управления доступом и информационными потоками в компьютерных системах; использовать основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
	Владеет	методами разработки частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками

Для формирования вышеуказанных компетенций в рамках дисциплины «Архитектура персонального компьютера» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Теория информации»

Рабочая программа учебной дисциплины «Теория информации» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.31.

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 академических часов. Учебным планом предусмотрены лекционные занятия (36 часов), лабораторные занятия (18 часов), практические занятия (18 часов), самостоятельная работа студента (36 часов). Дисциплина реализуется на 3 курсе в 6 семестре. Форма контроля по дисциплине – зачет.

Дисциплина базируется на предварительном изучении таких дисциплин, как «Математический анализ», «Введение в алгебру», «Информатика».

Дисциплина "Теория информации" обеспечивает получение базиса в области изучения фундаментальных положений теории информации, ознакомление с основными подходами к определению количественной меры информации, информационных пределов избыточности; изучение вопроса передачи непрерывной информации с оценкой ошибок дискретизации по времени и по амплитуде; исследовать возможность информационного подхода к оценке качества функционирования информационных систем. Получить необходимый минимум сведений о каналах связи, помехах, методах построения кодирующих и декодирующих устройств, информационных носителях, способах сжатия и хранения информации. Содействует фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Цель дисциплины - обучить студентов основам теории информации, обрести навыки вероятностного математического анализа дискретных и непрерывных последовательностей случайных величин, содержащих

информацию, научить решать задачи эффективного, а также помехозащитного кодирования/декодирования.

Задачи дисциплины:

- дать основы теоретико-вероятностных подходов в определении количества информации;
 - дать основы методологии создания эффективного и/или помехозащитного кода;
 - дать основы процессов сжатия и восстановления информации.
- получить представление о методах кодирования, овладеть методикой построения кодов, получить практику безызбыточного кодирования и ознакомиться с методами построения эффективных кодов, оптимальных с точки зрения минимальной средней длины кодовых слов.

Для успешного изучения дисциплины «Теория информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций).

Код и формулировка	Этапы формирования компетенции
--------------------	--------------------------------

компетенции		
(ОПК-2) способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Знает	фундаментальные положения теории информации; методы формализации и представления знаний в информационных системах.
	Умеет	использовать подходы к количественной мере информации; рассчитывать скорость передачи информации и пропускная способность канала связи при отсутствии и наличии помех.
	Владеет	навыками использования численных методов для решения стандартных вычислительных задач.

Для формирования вышеуказанных компетенций в рамках дисциплины «Теория информации» применяются следующие методы активного/интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: лабораторные работы (ПР-6), собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Компьютерные сети»

Данный курс предназначен студентам по направлению подготовки 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.33.

Трудоемкость дисциплины в зачетных единицах составляет 3 з.е., в академических часах – 108 часов (лекции – 36 часов, лабораторная работа – 30 часа, практические занятия – 4 часов, самостоятельная работа – 36 часов). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Компьютерные сети» базируется на предварительном изучении следующих дисциплин: «Математическая логика и теория алгоритмов», «Методы программирования», «Операционные системы», «Аппаратные средства вычислительной техники», что обеспечивает лучшее усвоение материала и дает целостную картину о современном состоянии и развитии компьютерной техники.

Данная дисциплина затрагивает такие вопросы, как основные методы организации взаимодействия между составными частями компьютерных сетей, тенденции дальнейшего их развития, а также некоторые элементы конфигурирования и администрирования локальных компьютерных сетей.

Цель дисциплины – ознакомить студентов основными принципами функционирования компьютерных сетей и систем передачи данных.

Задачи дисциплины:

- знакомство с современными представлениями о компьютерных сетях, их архитектурой, моделями, протоколами и аппаратным обеспечением;
- изучить основные методы организации взаимодействия между составными частями компьютерных сетей, тенденциями дальнейшего их развития, а также с некоторыми элементами конфигурирования и

администрирования локальных компьютерных сетей.

Для успешного изучения дисциплины «Компьютерные сети» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

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

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

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-7) способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с	Знает	историю развития компьютерных сетей и систем передачи данных. современные тенденции развития компьютерных сетей. принципы преобразования информации в компьютерной сети.
	Умеет	быстро адаптироваться к обновлениям компьютерных сетей и систем передачи данных. подключать дополнительное оборудование и настраивать связь между элементами компьютерной

программными средствами общего и специального назначения		сети.
	Владеет	навыком самостоятельно создать компьютерную сеть из нескольких компьютеров. навыком самостоятельно производить настройку программного обеспечения компьютерной сети.

Для формирования вышеуказанных компетенций в рамках дисциплины «Компьютерные сети» применяются следующие методы активного/интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: лабораторные работы (ПР-6), собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Защита в операционных системах»

Рабочая программа дисциплины «Защита в операционных системах» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.34.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов (лекции – 36 часов, практические занятия – 4, лабораторные занятия – 32 часов, самостоятельная работа – 36 часов). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – зачет.

Дисциплина логически и содержательно связана с такими курсами, как «Информатика», «Математическая логика и теория алгоритмов», «Основы информационной безопасности», «Операционные системы».

Дисциплина имеет теоретическую направленность, при этом большое значение для освоения дисциплины имеют лабораторные занятия, в ходе которых студенты получают знания и навыки использования объектов ядра операционной системы, практически используют возможности модели безопасности операционной системы.

Цель дисциплины: формирование у студентов навыков, необходимых для решения следующих профессиональных задач.

Задачи:

- изучить основные задачи операционных систем, основные концепции современных операционных систем;
- изучить встроенные средства безопасности в операционных системах;
- изучить стандарты защищенности операционных систем;
- изучить средства идентификация, аутентификация и авторизация;
- поиск рациональных решений при разработке средств защиты информации с учетом требований качества;
- изучить программные средства для решения административных задач;

- обеспечение эффективного функционирования средств защиты информации с учетом требований по обеспечению защищенности системы.

Для успешного изучения дисциплины «Защита в операционных системах» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);
- способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);
- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);
- способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-3 способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных	Знает	офисные технологии и специальное программное обеспечение при работе с современными операционными системами.
	Умеет	анализировать полученную информацию, синтезировать и осмысливать полученную информацию.
	Владеет	навыками анализа и составления отчетных документов.

фондах и иных источниках информации		
ОПК-7 способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Знает	интернет-технологии для поиска информации.
	Умеет	использовать пакеты прикладных программ для решения задач профессиональной деятельности.
	Владеет	навыками работы с прикладными программами. навыками анализа эффективности используемых прикладных программ.
ОПК-8 способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Знает	интернет-технологии для поиска информации.
	Умеет	использовать пакеты прикладных программ для решения задач профессиональной деятельности.
	Владеет	навыками работы с прикладными программами. навыками анализа эффективности используемых прикладных программ.

Для формирования вышеуказанных компетенций в рамках дисциплины «Защита в операционных системах» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: курсовая работа (ПР-5), собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Основы построения защищенных компьютерных сетей»

Данный курс предназначен студентам по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.35.

Общая трудоёмкость дисциплины в зачетных единицах составляет 144 часа (4 з.е.). Учебным планом предусмотрены лекционные занятия – 36 часов, лабораторные работы – 4 часа, практическая работа – 32 часа, самостоятельная работа студентов – 45 часов. Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Основы построения защищенных компьютерных сетей» базируется на предварительном изучении следующих дисциплин: «Языки программирования», «Операционные системы», «Сети и системы передачи информации», «Основы информационной безопасности».

Дисциплина является базовой для изучения курсов по телекоммуникационным сетям. Знания, умения и практические навыки, полученные в результате изучения дисциплины «Основы построения защищенных компьютерных сетей», позволят студентам основывать свою профессиональную деятельность на построении, проектировании и эксплуатации программно-аппаратных технологий защиты передачи информации.

Цель дисциплины: изучение методов и средств построения и эксплуатации беспроводных технологий для обеспечения информационной безопасности на объекте, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий защиты передачи информации в беспроводных коммуникациях.

Задачи:

- разработка проектов систем и подсистем защищенных компьютерных сетей в соответствии с техническим заданием;

- проведение инструментального мониторинга защищенности объекта;
- поиск рациональных решений при разработке средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения;
- установка, настройка, эксплуатация и обслуживание аппаратно-программных средств защиты информации;
- обеспечение эффективного функционирования средств защиты информации с учетом требований по обеспечению защищенности компьютерной системы.

Для успешного изучения дисциплины «Основы построения защищенных компьютерных сетей» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);
- способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции		
ОПК-7 способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Знает		интернет-технологии для поиска информации.
	Умеет		использовать пакеты прикладных программ для решения задач профессиональной деятельности.
	Владеет		навыками работы с прикладными программами. навыками анализа эффективности используемых прикладных программ.
ОПК-8 способность	Знает		интернет-технологии для поиска информации.

использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Умеет	использовать пакеты прикладных программ для решения задач профессиональной деятельности.
	Владеет	навыками работы с прикладными программами. навыками анализа эффективности используемых прикладных программ.
ПК-3 способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знает	методы сбора и анализа данных при проектировании системы защиты компьютерной сети.
	Умеет	выявлять различные типы проблемных ситуаций.
	Владеет	навыками анализа и составления отчетных документов.

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы построения защищенных компьютерных сетей» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Основы построения защищённых баз данных»

Курс учебной дисциплины «Основы построения защищенных баз данных» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.36.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов (лекции – 36 часов, практические занятия – 32 часа, самостоятельная работа – 36 часов, лабораторная работа – 4 часа). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – зачёт.

Дисциплина логически и содержательно связана с такими курсами, как «Языки программирования», «Системы управления базами данных», «Основы информационной безопасности».

Дисциплина является базовой для изучения курсов по телекоммуникационным сетям. Знания, умения и практические навыки, полученные в результате изучения дисциплины «Основы построения защищенных баз данных», позволят студентам основывать свою профессиональную деятельность на построении, проектировании и эксплуатации программно-аппаратных технологий защиты передачи информации.

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

Задачи:

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

Для успешного изучения дисциплины «Основы построения защищенных баз данных» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные/ профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-8 – способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Знает	интернет-технологии для поиска информации
	Умеет	использовать пакеты прикладных программ для решения задач профессиональной деятельности
	Владеет	навыками работы с прикладными программами, навыками анализа эффективности используемых прикладных программ
ПК-17 – способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	Знает	методы сбора и анализа данных при проектировании системы защиты компьютерной сети
	Умеет	производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение
	Владеет	навыком выявления различных типов проблемных ситуаций, навыками анализа и составления отчетных документов

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы построения защищенных баз данных» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Защита программ и данных»

Рабочая программа учебной дисциплины «Защита программ и данных» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в базовую часть дисциплин учебного плана Б1.Б.37.

Трудоемкость дисциплины в зачетных единицах составляет 7 з.е., в академических часах – 252 часа (лекции – 28 час., лабораторные работы – 84 час., самостоятельная работа – 140 час.). Дисциплина реализуется на 5 курсе в А семестре. Форма контроля по дисциплине – экзамен, зачет.

Дисциплина «Защита программ и данных» базируется на предварительном изучении таких курсов, как «Операционные системы» и «Основы информационной безопасности».

Курс лекций дисциплины построен на пошаговом повествовании от методов, технологий и программного обеспечения для защиты программ к основным принципам.

Цель дисциплины – знакомство с основными методами и средствами обеспечения защиты исполнимых файлов при разработке и использовании программного обеспечения, и методами защиты данных.

Задачи:

- знакомство с основными методами обеспечения защиты исполнимых файлов при разработке программного обеспечения;
- знакомство с основными программными средствами обеспечения защиты исполнимых файлов;
- знакомство с основными методами защиты данных.

Для успешного изучения дисциплины «Защита программ и данных» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и

обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);

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

- способность использовать нормативные правовые документы в своей профессиональной деятельности (ОПК-5);

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-7) способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Знает	методы и технологии защиты информации, основные понятия, категории и инструменты анализа систем обеспечения безопасности.
	Умеет	использовать internet-ресурсы, полнотекстовые баз данных и каталогов, электронные журналы и патенты, поисковые ресурсы для поиска информации в области информационной безопасности.
	Владеет	основными приемами анализа технологии выполнения наиболее типичных операций применительно к сфере своей деятельности.
(ОПК-8) способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Знает	современные языки программирования и программные комплексы.
	Умеет	строить алгоритмы.
	Владеет	навыком самостоятельного построения алгоритма, проведения его анализа и реализации в современных программных комплексах.

Для формирования вышеуказанных компетенций в рамках дисциплины «Защита программ и данных» применяются следующие методы обучения: чтение лекций с использованием мультимедийного оборудования (проектор), проведение и сдача лабораторных работ. Используемые оценочные средства:

конспект (ПР-7), лабораторные работы (ПР-6).

Аннотация к рабочей программе дисциплины «Сети и системы передачи информации»

Курс учебной дисциплины «Сети и системы передачи информации» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.38.

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 академических часов. Учебным планом предусмотрены лекции (36 часов), практические занятия (36 часа), самостоятельная работа студента (63 часа, в том числе 45 часов на подготовку к экзамену). Дисциплина реализуется на 3 курсе в 6 семестре. Форма контроля по дисциплине – экзамен.

Преподавание курса основано на предварительном изучении студентами курсов «Основы информационной безопасности», «Методы программирования».

Курс лекций строится на пошаговом повествовании от основных терминов в области компьютерных сетей к изучению архитектур LAN и Ethernet, и протоколам среднего уровня.

Цель курса - ознакомить студентов с современными представлениями о компьютерных сетях, их архитектурой, моделями, протоколами и аппаратным обеспечением.

Задачи:

- создать теоретическую и практическую базу для постановки и решения задач в области связи;
- изучить основные методы организации взаимодействия между составными частями компьютерных сетей, тенденциями дальнейшего их развития, а также с некоторыми элементами конфигурирования и администрирования локальных компьютерных сетей;

- создать основу для взаимодействия со специалистами различных специальностей при проектировании, разработке, организации эксплуатации систем и сетей связи.

Для успешного изучения дисциплины «Сети и системы передачи информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8);
- способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-3 – способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	Знать	методы и технологии защиты информации, основные понятия, категории и инструменты анализа систем обеспечения безопасности
	Уметь	использовать Интернет-ресурсы, полнотекстовые баз данных и каталогов, электронные журналы и патенты, поисковые ресурсы для поиска информации
	Владеть	основными приемами анализа, технологии выполнения наиболее типичных операций применительно к сфере своей деятельности

ОПК-7 – способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Знает	основы Интернет-технологий; типовые структуры и принципы организации компьютерных сетей
	Умеет	уметь работать с современным сетевым программным обеспечением: клиентскими программами протокола передачи файлов, клиентскими программами удаленного администрирования, электронной почтой, вспомогательными программами сетевых служб
	Владеет	владеть приемами и навыками передачи данных, а также техникой настройки сетевого программного обеспечения персональных компьютеров

Для формирования вышеуказанных компетенций в рамках дисциплины «Сети и системы передачи информации» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), тест (ПР-1), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Теория кодирования, сжатия и восстановления информации»

Курс учебной дисциплины «Теория кодирования, сжатия и восстановления информации» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.40.1.

Общая трудоемкость курса 5 зачетных единиц, 180 академических часов. Учебным планом предусмотрены лекционные занятия (36 часов), практические занятия (54 часа), самостоятельная работа (27 часа, в том числе 63 часов на подготовку к экзамену). Дисциплина реализуется на 4 курсе 8 семестра. Форма контроля по дисциплине – экзамен.

Дисциплина «Теория кодирования, сжатия и восстановления информации» предполагает предварительное освоение дисциплин «Дискретная математика», «Теория вероятностей и математическая статистика», «Теория информации».

В курсе рассматриваются математические основы для понимания основных понятий, теорем и алгоритмов буквенного кодирования. Даются алгебраические основы теории линейного кодирования, на основе которых строится теория кодов, исправляющих одну и две ошибки. Даются алгоритмы декодеров и кодеров для таких кодов, а также алгоритмы для взаимно-однозначных кодов с минимальной избыточностью.

Цель – формирование компетенций обучающихся в области построения и исследования различных дискретных кодов.

Задачи:

- сформировать теоретическое понимание принципов дискретного кодирования;
- дать практические основы построения дискретных кодов и методов исследования их свойств.

Для успешного изучения дисциплины «Теория кодирования, сжатия и восстановления информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

В результате изучения данной дисциплины у обучающихся формируются следующие профессионально-специализированные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
ПСК-2.1 – способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает	стандартные алгоритмы применяемых методов и методов обработки результатов
	Умеет	проводить научные эксперименты, обрабатывать результаты эксперимента и анализировать полученные результаты
	Владеет	компьютерными пакетами для проведения исследовательских экспериментов, обработки и анализа результатов
ПСК-2.2 – способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знает	методы анализа и обоснования адекватности математических процессов, возникающих при работе программно-аппаратных средств защиты информации
	Умеет	разрабатывать, анализировать и обосновывать адекватность математических моделей процессов
	Владеет	навыком разработки, анализа и обоснования адекватности математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации
ПСК-2.4 – способностью разрабатывать, анализировать и обосновывать адекватность математических	Знает	основные алгоритмы эллиптической криптографии
	Умеет	моделировать алгоритмы в системах компьютерной математики, оценивать эффективность
	Владеет	навыком моделирования алгоритмов. Методами оценивания их работоспособности и

моделей процессов, возникающих при работе программно-аппаратных средств защиты информации		эффективности
-------------------------------------------------------------------------------------------	--	---------------

Для формирования вышеуказанных компетенций в рамках дисциплины «Теория кодирования, сжатия и восстановления информации» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Теория псевдослучайных генераторов»

Курс учебной дисциплины «Теория псевдослучайных генераторов» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.40.2.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единицы, 180 часов. Учебным планом предусмотрены лекционные занятия (36 часов), лабораторные работы (8 часов), практические занятия (64 часов), самостоятельная работа (18 часа, в том числе 54 часов на подготовку к экзамену). Дисциплина реализуется на 4 курсе, в 8 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Теория псевдослучайных генераторов» основана на предварительном изучении следующих дисциплин: «Математическая логика и теория алгоритмов», «Алгебра», «Теория вероятностей и математическая статистика», «Языки программирования».

Дисциплина «Теория псевдослучайных генераторов» обеспечивает приобретение знаний и умений в области алгоритма генератора псевдослучайных чисел, порождающего последовательность чисел, элементы которой подчиняются заданному распределению. Изучение этой дисциплины способствует освоению принципов применения генератора псевдослучайных чисел в информатике – от метода Монте-Карло и имитационного моделирования до криптографии.

Цель: подготовка к научно-исследовательской деятельности в областях, использующих математические методы и компьютерные технологии.

Задачи:

- изучить основные определения и понятия теории псевдослучайных генераторов;

- подготовка к работе, связанной с решением различных задач, предполагающих использование математического моделирования процессов и объектов и программного обеспечения;
- подготовка к работе в сфере защиты информации.
- изучить основные способы построения псевдослучайных генераторов;
- разрабатывать и анализировать математические модели процессов с использованием генератора псевдослучайных чисел.

Для успешного изучения дисциплины «Теория псевдослучайных генераторов» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);
- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4).

В результате изучения данной дисциплины у обучающихся формируются следующие профессионально-специализированные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
ПСК-2.1 – способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает	принципы построения и свойства псевдослучайных генераторов
	Умеет	составлять конспект по изучаемому материалу, делать выводы в ходе выполнения практических заданий
	Владеет	основными знаниями в области теории псевдослучайных генераторов
ПСК-2.2 – способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и	Знает	основные определения и понятия теории псевдослучайных генераторов
	Умеет	формулировать результат проведенных исследований в ходе выполнения практических заданий

методов защиты информации в компьютерных системах	Владеет	основными терминами предметной области
ПСК-2.4 – способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знает	основные способы построения псевдослучайных генераторов
	Умеет	научно и практически обосновано излагать результаты исследований
	Владеет	основными знаниями в построении псевдослучайных генераторов

Для формирования вышеуказанных компетенций в рамках дисциплины «Теория псевдослучайных генераторов» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Методы алгебраической геометрии в криптографии»

Курс учебной дисциплины «Методы алгебраической геометрии в криптографии» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.40.3.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 часов (лекции – 36 часов, лабораторные занятия – 8 часов, практическая работа – 64 часа, самостоятельная работа – 27 часов, в том числе 45 часов на подготовку к экзамену). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина логически и содержательно связана с такими курсами, как «Алгебра», «Геометрия», «Дискретная математика», «Теория вероятностей и математическая статистика», «Теория информации», «Математическая логика и теория алгоритмов», «Методы программирования» и «Теоретико-числовые методы в криптографии».

Курс «Методы алгебраической геометрии в криптографии» составляет одну из фундаментальных частей современной теоретической криптографии, без знания которых невозможна дальнейшая профессиональная подготовка в области современной защиты информации. При освоении данного курса у студентов формируются навыки грамотного применения теоретических основ криптографии в постановке практических задач, в решении задач с применением современного теоретического аппарата, в систематизации полученных знаний.

Цель: выработать у студентов умения применять основные приёмы геометрических методов при исследовании математических моделей, возникающих в естествознании и прикладных науках, развить математическую культуру студента и подготовить его к усвоению других основных математических курсов.

Задачи:

- последовательное изложение теоретического материала на лекциях, при котором все основные результаты снабжаются строгими доказательствами;
- сформировать представление о комплексе идей и методов классической геометрии плоскости и пространства;
- отработка приемов решения задач на практических занятиях.

Для успешного изучения дисциплины «Методы алгебраической геометрии в криптографии» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);
- способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3).

В результате изучения данной дисциплины у обучающихся формируются следующие профессионально-специализированные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
ПСК-2.2 – способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знает	методы алгебраической геометрии в криптографии
	Умеет	оценивать эффективность средств и методов защиты информации в компьютерных системах
	Владеет	методами алгебраической геометрии в криптографии

ПСК-2.3 – способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	Знает	методы алгебраической геометрии в криптографии
	Умеет	разрабатывать алгоритмы, реализующие современные математические методы защиты информации
	Владеет	методами алгебраической геометрии в криптографии
ПСК-2.5 – способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации	Знает	методы алгебраической геометрии в криптографии
	Умеет	оценивать эффективность средств защиты информации
	Владеет	методами алгебраической геометрии в криптографии

Для формирования вышеуказанных компетенций в рамках дисциплины «Методы алгебраической геометрии в криптографии» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Дополнительные главы математической статистики»

Данный курс предназначен студентам, обучающимся по направлению подготовки 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав обязательных дисциплин вариативной части учебного плана Б1.В.ОД.2.

Трудоемкость дисциплины в зачетных единицах составляет 3 з.е., в академических часах – 108 часа (лекции – 36 часов, практическая работа – 16 часов, лабораторная работа – 2 часа, самостоятельная работа – 54 часов). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Дополнительные главы математической статистики» базируется на предварительном изучении следующих дисциплин: «Математический анализ», «Введение в алгебру», «Основы геометрии», «Теория вероятностей и математическая статистика».

Дисциплина является продолжением курса «Теория вероятностей и математическая статистика». В рамках этого курса предлагается рассмотреть такие его разделы, как теория массового обслуживания и теория игр. На момент изучения дисциплины студент должен обладать умением дифференцировать и интегрировать, иметь понимание основных концепций математического анализа и теории функций комплексного переменного, владеть матричной алгеброй, уметь работать с электронными таблицами.

Цель – ознакомить студентов с основами теории вероятности, а также с методами решения вероятностных задач в физике и других областях приложения теории вероятности.

Задачи:

- научиться работать со случайными событиями, оценивать их шансы, принимать решения по результатам экспериментальных данных;
- научиться строить математические модели реальных процессов с учетом случайности рассматриваемых величин.

Для успешного изучения дисциплины «Дополнительные главы математической статистики» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-2) способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Знает	основные понятия и определения математической статистики, используемые для решения различных задач и обработки экспериментальных данных. математический аппарат современной теории вероятности математической статистики.
	Умеет	применять основные формулы математической статистики и законы теории вероятностей для решения стандартных задач. выявлять естественную сущность проблем, возникающих в ходе профессиональной деятельности, и применять основные формулы математической статистики для их формализации, анализа и выработки решения.
	Владеет	навыком вычисления вероятности событий. навыком применения основных формул математической статистики для решения стандартных задач.
(ПК-19) способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Знает	технические средства защиты и их устройство; методы анализа для нахождения неисправностей.
	Умеет	производить проверку технического состояния средств защиты.
	Владеет	навыком обращения со средствами технической защиты информации

Для формирования вышеуказанных компетенций в рамках дисциплины «Дополнительные главы математической статистики» применяются следующие методы активного/интерактивного обучения: интерактивные и

проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7), лабораторная работа (ПР-6).

Аннотация к рабочей программе дисциплины «Дополнительные главы криптографических протоколов»

Курс учебной дисциплины «Дополнительные главы криптографических протоколов» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в обязательные дисциплины вариативной части учебного плана Б1.В.ОД.4.

Трудоёмкость дисциплины составляет 144 академических часа (4 з.е). Учебным планом предусмотрены лекционные занятия 28 часов, практические занятия 42 часа, самостоятельная работа студента 74 часов. Дисциплина реализуется на 5 курсе в А семестре. Форма контроля по дисциплине – зачёт.

Изучение дисциплины базируется на курсах: «Криптографические методы защиты информации», «Криптографические протоколы», «Теоретико-числовые методы в криптографии».

Содержание дисциплины охватывает следующий круг вопросов: стандарты на цифровую подпись и функцию хеширования, специфические криптографические протоколы, практические криптографические протоколы, особенности применения криптографических алгоритмов на ИК.

Цель дисциплины «Дополнительные главы криптографических протоколов» заключается в углубленном изложении принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи:

- дать общие представления об эллиптических кривых над конечными полями;
- изучить криптографических особенностях применения интеллектуальных карт и специфических криптографических протоколов.

Для успешного изучения дисциплины «Дополнительные главы криптографических протоколов» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность осваивать методики использования программных средств для решения практических задач (ОПК-2);
- способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способность использовать нормативные правовые документы в своей профессиональной деятельности (ОПК-5);
- способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9);
- способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ОПК-10).

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-5) способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает	защитные механизмы и средства обеспечения безопасности операционных систем, средства и методы хранения и передачи аутентификационной информации, требования к подсистеме аудита и политике аудита, основные средства и методы анализа программных реализаций.
	Умеет	формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе, корректно применять симметричные и асимметричные криптографические алгоритмы.
	Владеет	навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств, навыками анализа программных реализаций.
(ПК-10) способность	Знает	основные виды симметричных и

оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		асимметричных криптографических алгоритмов, защитные механизмы и средства обеспечения безопасности операционных систем, средства и методы хранения и передачи аутентификационной информации, требования к подсистеме аудита и политике аудита. основные средства и методы анализа программных реализаций.
	Умеет	использовать средства защиты, предоставляемые системами управления базами данных, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях.
	Владеет	методиками анализа сетевого трафика, методиками анализа результатов работы средств обнаружения вторжений, навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств, навыками настройки межсетевых экранов.

Для формирования вышеуказанных компетенций в рамках дисциплины «Дополнительные главы криптографических протоколов» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Защита информации от технической разведки»

Рабочая программа учебной дисциплины «Защита информации от технической разведки» разработана для студентов по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в обязательную дисциплины вариативной части учебного плана Б1.В.ОД.5.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 академических часов. Учебным планом предусмотрены лекционные занятия (42 часа), лабораторные работы (14 часов), практические занятия (14 часов), самостоятельная работа (56 часов). Дисциплина реализуется на 5 курсе, в А семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Защита информации от технической разведки» основана на предварительном изучении следующих дисциплин: «Информатика», «Основы информационной безопасности», «Модели безопасности компьютерных систем», «Аппаратные средства вычислительной техники», «Защита программ и данных». Знания и практические навыки, полученные при изучении дисциплины «Защита информации от технической разведки», обеспечивают освоение следующих дисциплин: «Инженерная защита и охрана объектов», «Программно-аппаратные средства обеспечения информационной безопасности», «Теория и проектирование защищенных систем».

Дисциплина имеет практическую направленность, при этом большое значение для освоения дисциплины имеют лабораторные занятия. В ходе реализации дисциплины в рамках лекционных, лабораторных и практических занятий применяются методы активного/ интерактивного обучения, реализующие наглядное представление результатов защиты информации от технической разведки. Дисциплина «Защита информации от технической разведки» обеспечивает приобретение знаний и умений в области технической

разведки, а также обеспечения защиты информации от средств технической разведки. Изучение этой дисциплины способствует освоению способов и средств защиты выявленных каналов добывания информации.

Цель дисциплины – раскрыть природу ведения технической разведки, сформировать представление о проблемах защиты информации от технической разведки, выработать умения и навыки применению средств защиты информации от технической разведки, сформировать умения по выработке рекомендаций по защите от технической разведки.

Задачи:

- изучить основных угроз безопасности информации и модели нарушителя в КС;
- изучить основные этапы и процедуры добывания информации технической разведки;
- освоить методы спектрального анализа с помощью пакета прикладных программ MATLAB;
- изучить методы работы с комплексом выявления технических каналов утечки информации;
- изучить возможность выявления каналов утечки информации нелинейным локатором NR-900EM;
- оценить защищенность информации, обрабатываемой ТСПИ, от утечки по каналу ПЭМИ.

Для успешного изучения дисциплины «Защита информации от технической разведки» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

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

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

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

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-12) способность проводить инструментальный мониторинг защищенности компьютерных систем	Знает	особенности каналов утечки информации в компьютерных системах, методы и технические перекрытия этих каналов.
	Умеет	анализировать каналы утечки информации, возможные в конкретной компьютерной системе, организовывать защиту информации в ней.
	Владеет	программными и техническими средствами защиты информации в компьютерных системах.
(ПК-14) способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Знает	организационные, программные и технические методы защиты информации.
	Умеет	анализировать уровень защищённости информации в различных её проявлениях с привязкой к конкретным реальным условиям.
	Владеет	методами и практическими навыками анализа создания систем защиты информации.
(ПК-20) способность выполнять работы по восстановлению	Знает	методы технической и программной защиты информации.
	Умеет	тестировать конкретные компьютерные системы с

работоспособности средств защиты информации при возникновении нештатных ситуаций		использованием аппаратных и программных средств на предмет уровня защищённости информации в них и в помещениях где они расположены.
	Владеет	программными и аппаратными средствами контроля защиты информации

Для формирования вышеуказанных компетенций в рамках дисциплины «Защита информации от технической разведки» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Теория и проектирование защищенных систем»

Рабочая программа учебной дисциплины «Теория и проектирование защищенных систем» разработана для студентов, обучающихся по направлению подготовки 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в обязательную дисциплины вариативной части учебного плана Б1.В.ОД.6.

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 академических часа. Учебным планом предусмотрены лекции (50 часов), лабораторные работы (34 часа), самостоятельная работа студента (54 часа). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – зачет.

Изучение дисциплины «Теория и проектирование защищенных систем» базируется на следующих дисциплинах: «Информатика», «Основы информационной безопасности», «Компьютерные сети», «Аппаратные средства вычислительной техники».

В курс лекций включены такие темы как: «Основные понятия и определения», «Проектирование систем в защищенном исполнении», «Модели угроз», «Создание систем защиты персональных данных», «Основные категории средств защиты ИСПДн» и др.

Цель – изучение основных понятий, методологии и практических приемов проектирования, разработки и внедрения автоматизированных систем на предприятиях различных отраслей промышленности с учетом требований по обеспечению информационной безопасности

Задачи:

- приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в области защиты автоматизированных систем;

- формирование у обучаемых целостного представления об организации и содержании процессов проектирования, разработки, внедрения и эксплуатации автоматизированных систем (АС) в защищенном исполнении.

Для успешного изучения дисциплины «Теория и проектирование защищенных систем» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

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

- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);

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

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

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

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-6) способность участвовать в разработке проектной и технической документации	Знает	основную проектную и рабочую техническую документацию, стандарты, технические условия и другие нормативные документы.
	Умеет	находить необходимую информацию и исходные данные в стандартах, технических условиях и других нормативных документах.
	Владеет	навыками оформления законченных проектно-конструкторских работ.
(ПК-7) способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем	Знает	основные понятия проектирования защищенных компьютерных систем.
	Умеет	проводить анализ проектного решения по обеспечению защищенности компьютерных сетей.
	Владеет	навыками анализа проектного решения по обеспечению защищенности компьютерных сетей.
(ПК-8) способность участвовать в разработке подсистемы информационной безопасности компьютерной системы	Знает	основы предметной области: знать основные определения и понятия.
	Умеет	решать задачи предметной области: решать типовые задачи по предложенным методам и алгоритмам, в том числе с использованием компьютерных математических программ. графически иллюстрировать задачу. оценивать достоверность полученного решения.
	Владеет	математическим языком предметной области: основными терминами, понятиями, определениями разделов математического анализа. основными способами представления математической информации (аналитическим, графическим, символьным, словесным и др.).

Для формирования вышеуказанных компетенций в рамках дисциплины «Теория и проектирование защищенных систем» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Основы экономической безопасности»

Рабочая программа учебной дисциплины «Основы экономической безопасности» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в обязательную дисциплины вариативной части учебного плана Б1.В.ОД.7.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Учебным планом предусмотрены лекционные занятия (32 часов), практические занятия (2 часов), лабораторные работы (2 часа), самостоятельная работа (36 часов). Дисциплина реализуется на 5 курсе в 9-м семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Основы экономической безопасности» основана на предварительном изучении следующих дисциплин: «Экономика», «Информатика», «Основы информационной безопасности», «Основы управленческой деятельности», «Политология», «Организационное и правовое обеспечение информационной безопасности». Знания и практические навыки, полученные при изучении дисциплины «Основы экономической безопасности», обеспечивают освоение следующих дисциплин: «Охрана интеллектуальной собственности», «Инженерная защита и охрана объектов».

Дисциплина имеет теоретическую направленность, при этом большое значение для освоения дисциплины имеют как лекционные, так и практические занятия. В ходе реализации дисциплины в рамках лекционных и практических занятий применяются методы активного/ интерактивного обучения, реализующие наглядное представление об основах экономической безопасности. Дисциплина «Основы экономической безопасности» обеспечивает приобретение знаний и умений в области обеспечения экономической безопасности государства, организации. Изучение этой дисциплины способствует освоению основных понятий, методов оценки,

угроз и критериев экономической безопасности.

Цель дисциплины: ознакомить студентов с важнейшими аспектами экономической безопасности, сформировать представление о системе экономической безопасности государства, включающей экономическую безопасность регионов, экономическую безопасность хозяйствующих субъектов и личности, обучить студентов принципам обеспечения экономической безопасности государства, организации.

Задачи:

- изучить основные понятия экономической безопасности, критерии экономической безопасности предприятия;
- изучить угрозы экономической безопасности;
- изучить правовое обеспечение экономической безопасности;
- сформировать представление о роли и месте экономической безопасности в системе безопасности государства.
- применять методы оценки экономической безопасности.

Для успешного изучения дисциплины «Основы экономической безопасности» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- способность понимать социальную значимость своей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);
- способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6).

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные, профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ОК-2) способность использовать основы экономических знаний в различных сферах деятельности	Знает	основные нормативные правовые документы в области экономической безопасности.
	Умеет	анализировать угрозы экономической безопасности в финансово-банковской.
	Владеет	методами оценки и критериями экономической безопасности.
(ПК-1) способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	Знает	основные понятия и определения национальной безопасности.
	Умеет	анализировать угрозы в социальной сфере. приоритеты государственной социальной политики в стратегии экономической безопасности
	Владеет	инструментарием обеспечения экономической безопасности.

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы экономической безопасности» применяются следующие методы активного/интерактивного обучения: чтение лекций с использованием мультимедийного оборудования (проектор), проведение и сдача лабораторных работ, собеседование по итогам выполнения практических заданий.

Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Инженерная защита и охрана объектов»

Рабочая программа учебной дисциплины «Инженерная защита и охрана объектов» разработана для студентов по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в обязательную дисциплины вариативной части учебного плана Б1.В.ОД.8.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единицы, 180 часа. Учебным планом предусмотрены лекционные занятия (14 час), самостоятельная работа (28 час). Дисциплина реализуется на 5 курсе, в А семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Инженерная защита и охрана объектов» основана на предварительном изучении следующих дисциплин: «Физика», «Основы информационной безопасности», «Модели безопасности компьютерных систем», «Аппаратные средства вычислительной техники», «Защита программ и данных», «Электроника и схемотехника». Знания и практические навыки, полученные при изучении дисциплины «Инженерная защита и охрана объектов», обеспечивают освоение следующих дисциплин: «Защита информации от технической разведки», «Программно-аппаратные средства обеспечения информационной безопасности».

Дисциплина имеет теоретическую направленность, при этом большое значение для освоения дисциплины имеют, как лекционные, так и практические занятия. В ходе реализации дисциплины в рамках лекционных и практических занятий применяются методы активного/ интерактивного обучения, реализующие наглядное представление результатов инженерной защиты и охраны объектов. Дисциплина «Инженерная защита и охрана объектов» обеспечивает приобретение знаний и умений в области построения систем охраны и защиты. Изучение этой дисциплины способствует освоению особенностей и разновидностей (классификация) охранных систем, систем

управления доступом, методов и устройства идентификации.

Целью дисциплины является формирование у студентов знаний по основам инженерно-технической защите объектов, а также развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты объектов.

Задачи:

- изучить охранные и пожарные сигнализации, их классификации;
- изучить телеохранные системы сигнализации;
- изучить системы охранного телевидения;
- изучить системы управления доступом, их виды;
- научиться пользоваться терминологией, и методам решения задач, применяемым в области инженерно-технической защиты объектов.

Для успешного изучения дисциплины «Инженерная защита и охрана объектов» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность анализировать физические явления и процессы при решении профессиональных задач (ОПК-1);
- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения (ОПК-7);
- способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8);
- способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9).

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-9) способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы.	Знает	основные задачи, руководящие и нормативные документы систем охраны и защиты объектов
	Умеет	анализировать структуру систем охраны и защиты объектов
	Владеет	методами построения систем охраны и защиты объектов
(ПК-11) способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации.	Знает	общие принципы построения охраны и защиты объектов
	Умеет	использовать основные методы защиты систем охраны.
	Владеет	категориями средств защиты и охраны.
(ПК-12) способность проводить инструментальный мониторинг защищенности компьютерных систем.	Знает	современные тенденции развития информатики и вычислительной техники в области защиты и охраны объектов.
	Умеет	учитывать современные тенденции развития вычислительной техники в области защиты и охраны объектов при построении систем охраны и защиты объектов
	Владеет	навыками построения системы контроля доступом согласно современным тенденциям.

Для формирования вышеуказанных компетенций в рамках дисциплины «Инженерная защита и охрана объектов» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Программно-аппаратные средства обеспечения информационной безопасности»

Рабочая программа учебной дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» разработана для студентов, обучающихся по направлению подготовки 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в обязательные дисциплины вариативной части учебного плана Б1.В.ОД.9.

Общая трудоемкость освоения дисциплины составляет 7 зачетных единиц, 252 часа. Учебным планом предусмотрены лекционные занятия – 46 часов, лабораторные работы – 88 часов, самостоятельная работа – 64 часа, в том числе 54 часов на подготовку к экзамену. Дисциплина реализуется на 5 курсе, в 9 и А семестрах. Форма контроля по дисциплине в 9 семестре – зачет, в А семестре - экзамен.

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» основана на предварительном изучении следующих дисциплин: «Информатика», «Основы информационной безопасности», «Модели безопасности компьютерных систем».

Дисциплина имеет практическую направленность, при этом большое значение для освоения дисциплины имеют как лабораторные, так и лекционные занятия. В ходе реализации дисциплины в рамках лекционных и лабораторных занятий применяются методы активного/ интерактивного обучения, реализующие наглядное представление результатов использования программно-аппаратных средств обеспечения информационной безопасности. Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» обеспечивает приобретение знаний и умений в области средств обеспечения информационной безопасности программными и аппаратными средствами. Изучение этой дисциплины способствует освоению основных средств и методов защиты информации от

несанкционированного доступа с использованием аппаратно-программных средств; требований руководящих документов по защите информации от несанкционированного доступа.

Цель – сформировать представление о проблемах защиты информации в автоматизированных системах обработки информации; раскрыть природу явлений, заключающихся в нарушении целостности и конфиденциальности информации и дезорганизации работы компьютерных сетей; выработать умения и навыки применять основные методы и приемы защиты информации в автоматизированных системах, используя системы защиты информации и криптомаршрутизаторы.

Задачи:

- изучить требования руководящих документов по защите информации от несанкционированного доступа (НСД);
- изучить систему защиты информации от НСД;
- устанавливать, переустанавливать, удалять системы защиты информации;
- настраивать защитные механизмы систем защиты информации;
- составлять правила фильтрации криптомаршрутизатора.

Для успешного изучения дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);
- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);
- способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей

профессиональной деятельности, работать с программными средствами общего и специального назначения(ОПК-7);

- способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9);
- способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем(ПК-4).

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-5) способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает	особенности каналов утечки информации в компьютерных системах, методы и технические перекрытия этих каналов.
	Умеет	анализировать каналы утечки информации, возможные в конкретной компьютерной системе, организовывать защиту информации в ней.
	Владеет	программными и техническими средствами защиты информации в компьютерных системах.
(ПК-16) способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности	Знает	организационные, программные и технические методы защиты информации.
	Умеет	анализировать уровень защищённости информации в различных её проявлениях с привязкой к конкретным реальным условиям. составлять проекты нормативных правовых актов по комплексной защите информации.
	Владеет	методами и навыками анализа создания систем защиты информации.

компьютерных систем		
(ПК-18) способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает	методы технической и программной защиты информации.
	Умеет	тестировать конкретные компьютерные системы с использованием аппаратных и программных средств на предмет уровня защищённости информации в них и в помещениях, где они расположены.
	Владеет	программными и аппаратными средствами контроля защиты информации

Для формирования вышеуказанных компетенций в рамках дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Элективные курсы по физической культуре и спорту»

Рабочая программа учебной дисциплины «Элективные курсы по физической культуре и спорту» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин по выбору вариативной части учебного плана Б1.В.ДВ.

Общая трудоемкость освоения дисциплины составляет 328 академических часов. Учебным планом предусмотрены практические занятия (328 часов). Дисциплина реализуется на 1-3 курсах во 1, 2, 4, 5, 6 семестрах. Форма контроля по дисциплине – зачет.

Дисциплина «Элективные курсы по физической культуре и спорту» основана на предварительном изучении следующих дисциплин: «Безопасность жизнедеятельности», «Физическая культура».

Содержание дисциплины «Элективные курсы по физической культуре и спорту» предусматривает изучение техники, тактических взаимодействий, составляющими основу тактики игры; а также приобретение знаний, умений и навыков, необходимых для самостоятельной работы по изучаемым играм. Занятия проводятся в форме практических занятий. На практических занятиях студенты изучают технику и тактику игры, методику преподавания обучения и начальной подготовки. Овладевают необходимыми практическими умениями и навыками приемов техники и тактики, навыками игры. Учебная дисциплина «Элективные курсы по физической культуре и спорту» тесно связана не только с физическим развитием и совершенствованием функциональных систем организма молодого человека, но и с формированием средствами физической культуры и спорта жизненно необходимых психических качеств, свойств и черт личности.

Целью физического воспитания студентов является формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта и туризма для

сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей жизни и профессиональной деятельности.

Задачи:

- понимание социальной значимости физической культуры и её роли в развитии личности и подготовке к профессиональной деятельности;
- знание научно- биологических, педагогических и практических основ физической культуры и здорового образа жизни;
- формирование мотивационно-ценностного отношения к физической культуре, установки на здоровый стиль жизни, физическое совершенствование и самовоспитание привычки к регулярным занятиям физическими упражнениями и спортом;
- овладение системой практических умений и навыков, обеспечивающих сохранение и укрепление здоровья, психическое благополучие, развитие и совершенствование психофизических способностей, качеств и свойств личности, самоопределение в физической культуре и спорте;
- приобретение личного опыта повышения двигательных и функциональных возможностей, обеспечение общей и профессионально-прикладной физической подготовленности к будущей профессии и быту;
- создание основы для творческого и методически обоснованного использования физкультурно-спортивной деятельности в целях последующих жизненных и профессиональных достижений.

Для успешного изучения дисциплины «Элективные курсы по физической культуре и спорту» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-6).

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
(ОК-9) способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	Знает	правила и способы планирования индивидуальных занятий различной целевой направленности; влияние оздоровительных систем физического воспитания на укрепление здоровья, профилактику профессиональных заболеваний и вредных привычек
	Умеет	осуществлять творческое сотрудничество в коллективных формах занятий физической культурой; выполнять индивидуально подобранные комплексы оздоровительной и адаптивной (лечебной) физической культуры
	Владеет	способами контроля и оценки физического развития и физической подготовленности; навыками для организации и проведения индивидуального, коллективного отдыха

Для формирования вышеуказанных компетенций в рамках дисциплины «Элективные курсы по физической культуре» применяются следующие методы обучения: чтение лекций.

Аннотация к рабочей программе дисциплины «Системное программное обеспечение»

Курс учебной дисциплины «Системное программное обеспечение» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин выбора вариативной части учебного плана Б1.В.ДВ.4.1.

Общая трудоемкость дисциплины составляет 72 часа (2 з.е.). Учебным планом предусмотрены лекционные занятия (30 часов), лабораторные работы (2 часа), практические занятия (4 часа), самостоятельная работа студента (36 часов). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Системное программное обеспечение» логически и содержательно связана с такими курсами, как «Информатика», «Языки программирования», «Защита в операционных системах».

Содержание дисциплины охватывает следующий круг вопросов: основные понятия и термины дисциплины, системное программное обеспечение, классификация системных программ, Архитектура UNIX, интерфейс операционной системы, синхронизация потоков и др.

Целью дисциплины «Системное программное обеспечение» является изучение организации функционирования (алгоритмов функционирования ОС) вычислительных процессов в современных ЭВМ, комплексах и вычислительных системах.

Задачи дисциплины:

- освоение студентами системного программирования;
- приобретение навыков самостоятельного изучения отдельных тем дисциплины и решения типовых задач;
- приобретение навыков работы в современных интегрированных системах программирования для реализации программных продуктов;

- усвоение полученных знаний студентами, а также формирование у них мотивации к самообразованию за счет активизации самостоятельной познавательной деятельности.

Для успешного изучения дисциплины «Системное программное обеспечение» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

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

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

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

В результате изучения данной дисциплины у студентов формируются следующие профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-11) способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в	Знает	требования безопасности информации, предъявляемые средствам защиты информации в компьютерных системах;
	Умеет	оценивать различные web-сервисы с точки зрения безопасности информации;
	Владеет	опытом проведения экспериментально-исследовательских работ по оценке информационной безопасности web-сервисов

компьютерных системах по требованиям безопасности информации		
(ПК-15) способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Знает	требования, предъявляемые к системе управления информационной безопасностью компьютерной системы;
	Умеет	оценивать текущее состояние системы управления информационной безопасностью и выбирать наиболее эффективные методы по её совершенствованию:
	Владеет	методами и web-технологиями, необходимыми для совершенствования системы управления информационной безопасностью компьютерной системы.

Для формирования вышеуказанных компетенций в рамках дисциплины «Системное программное обеспечение» применяются следующие методы: чтение лекций, проведение и сдача лабораторных работ, собеседование по итогам выполнения практических заданий. Используемые оценочные средства: собеседование (ОУ-1), лабораторные работы (ЛР-6), конспект (ЛР-7).

Аннотация к рабочей программе дисциплины «Web-технологии»

Курс учебной дисциплины «Web-технологии» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин выбора вариативной части учебного плана Б1.В.ДВ.4.

Общая трудоемкость дисциплины составляет 72 часа (2 з.е.). Учебным планом предусмотрены лекционные занятия (36 часов), практические занятия (4 часа), самостоятельная работа студента (36 часов). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Web-технологии» логически и содержательно связана с такими курсами, как «Информатика», «Языки программирования», «Сети и системы передачи информации», «Компьютерные сети».

Содержание дисциплины охватывает следующий круг вопросов: история и основные тенденции развития Web-технологий, принципы гипертекстовой разметки и каскадные таблицы стилей CSS, языки JavaScript и динамический HTML, серверное программирование.

Цель изучения дисциплины «Web-технологии» - познакомить с базовыми концепциями и приемами web-программирования, научить использовать современные web-технологии.

Задачи:

- научить использовать современные web-технологии (CGI, Ajax);
- научить использовать современные языки для создания web-приложений (HTML, CSS, JavaScript);
- научить создавать web-сервисы, сайты, порталы с использованием этих технологий.

Для успешного изучения дисциплины «Web-технологии» у обучающихся должны быть сформированы следующие предварительные компетенции:

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

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

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

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

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-11) способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	Знает	требования безопасности информации, предъявляемые средствам защиты информации в компьютерных системах.
	Умеет	оценивать различные web-сервисы с точки зрения безопасности информации.
	Владеет	опытом проведения экспериментально-исследовательских работ по оценке информационной безопасности web-сервисов.
(ПК-15) способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Знает	требования, предъявляемые к системе управления информационной безопасностью компьютерной системы.

	Умеет	оценивать текущее состояние системы управления информационной безопасностью и выбирать наиболее эффективные методы по её совершенствованию.
	Владеет	методами и web-технологиями, необходимыми для совершенствования системы управления информационной безопасностью компьютерной системы.

Для формирования вышеуказанных компетенций в рамках дисциплины «Системное программное обеспечение» применяются следующие методы обучения: чтение лекций, проведение и сдача лабораторных работ, собеседование по итогам выполнения практических заданий. Используемые оценочные средства: собеседование (ОУ-1), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Интеллектуальные компьютерные системы»

Рабочая программа учебной дисциплины «Интеллектуальные компьютерные системы» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации и входит в состав дисциплин выбора вариативной части учебного плана Б1.В.ДВ.6.1.

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 академических часа. Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (32 час.), самостоятельная работа студента (9 час.). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина логически и содержательно связана с такими курсами, как «Дискретная математика», «Математическая логика и теория алгоритмов», «Теория вероятностей и математическая статистика», «Языки программирования», «Методы программирования». Данная дисциплина предназначена для ознакомления студентов с основными концепциями искусственного интеллекта (ИИ), моделями и методами представления знаний, подходами к обработке знаний.

В рамках курса рассматриваются основные понятия теории интеллектуальных систем – знания, информация, системы и подходы к представлению знаний с использованием вычислительной техники, понятия интеллектуальной деятельности. Рассматриваются как основополагающие концепции – поиск решения задач, представление знаний, алгоритмы интеллектуальных систем – так и специализированные области применения ИИ.

Цель данной дисциплины – дать систематический обзор современных моделей представления знаний, изучить и освоить принципы построения экспертных систем, рассмотреть перспективные направления развития систем

искусственного интеллекта и принятия решений.

Задачи:

- рассмотреть краткую историю становления и развития искусственного интеллекта;
- изложить технические постановки основных задач, решаемых системами искусственного интеллекта;
- познакомить с концепциями и методами, составляющими основу для понимания современных достижений искусственного интеллекта;
- ознакомить с современными областями исследования по искусственному интеллекту;
- ознакомить с основными моделями представления знаний и некоторыми интеллектуальными системами;
- познакомить с особенностями практического использования интеллектуальных информационных систем в области защиты информации.

Для успешного изучения дисциплины «Интеллектуальные компьютерные системы» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);
- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8).

В результате изучения данной дисциплины у обучающихся формируются

следующие профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-11) способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	Знает	теорию технологий искусственного интеллекта;
	Умеет	строить модели представления знаний;
	Владеет	подходами и техникой решения задач искусственного интеллекта, информационных моделей знаний, методами представления знаний.
(ПК-15) способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Знает	особенности создания и функционирования интеллектуальных систем обеспечения информационной безопасности;
	Умеет	оценивать текущее состояние интеллектуальной системы обеспечения информационной безопасности;
	Владеет	методами и технологиями, необходимыми для совершенствования интеллектуальной системы обеспечения информационной безопасности.

Для формирования вышеуказанных компетенций в рамках дисциплины «Интеллектуальные компьютерные системы» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: лабораторные работы (ПР-6), собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Модели знаний и онтологии»

Курс учебной дисциплины «Модели знаний и онтологии» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин выбора вариативной части учебного плана Б1.В.ДВ.6.2.

Трудоёмкость дисциплины в зачетных единицах составляет 108 часа (3 з.е.) Учебным планом предусмотрены лекционные занятия – 36 часов, лабораторные работы – 32 часов, практические занятия – 4 часа, самостоятельная работа студента – 36 часа, в том числе на подготовку к экзамену 27 часов. Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – экзамен.

Данный курс базируется на предварительном изучении дисциплин «Языки программирования», «Теория информации».

Содержание дисциплины охватывает следующий круг вопросов: данные, информация, знания, проблемы получения знаний, хранение знаний, онтологии и семантические сети, форматы и средства разработки онтологий.

Цель изучения дисциплины «Модели знаний и онтологии» заключается в получение студентами навыков применения моделей знаний и методов онтологического подхода в проектировании систем обработки знаний.

Задачи:

- изучение моделей знаний и их применения в информационных системах;
- освоение методик онтологического подхода для проектирования систем хранения знаний;
- понимание современных тенденций в области интеллектуальных систем.

Для успешного изучения дисциплины «Модели знаний и онтологии» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность осваивать методики использования программных средств для решения практических задач (ОПК-2);

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

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

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

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

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-11) способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	Знает	основные понятия стандартизации в области ИТ, основные национальные и международные стандарты в области ИТ.; методы оценки качества проекта и программных средств (базы данных, базы знаний); порядок и правила процедуры сертификации программной продукции, основы стандартизации и сертификации.
	Умеет	руководствоваться требованиями государственных стандартов в области ИТ в практической деятельности.; оформлять сопроводительную документацию к разработанному проекту средству, применять стандарты в области ИТ для обеспечения качества программных средств.

	Владеет	понятиями и факторами, определяющими качество проекта средств.
(ПК-15) способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Знает	основные понятия стандартизации в области ИТ, основные национальные и международные стандарты в области ИТ; методы оценки качества проекта и программных средств (базы данных, базы знаний); порядок и правила процедуры сертификации программной продукции, основы стандартизации и сертификации.
	Умеет	руководствоваться требованиями государственных стандартов в области ИТ в практической деятельности; оформлять сопроводительную документацию к разработанному проекту средству, применять стандарты в области ИТ для обеспечения качества программных средств.
	Владеет	понятиями и факторами, определяющими качество проекта средств.

Для формирования вышеуказанных компетенций в рамках дисциплины «Системное программное обеспечение» применяются следующие методы обучения: чтение лекций, проведение и сдача лабораторных работ, собеседование по итогам выполнения практических заданий. Используемые оценочные средства: собеседование (ОУ-1), лабораторные работы (ПР-6), конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Военная подготовка»

Курс учебной дисциплины «Военная подготовка» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав факультативных дисциплин учебного плана ФТД.1.

Общая трудоемкость освоения дисциплины составляет 432 часа (12 з.е.). Учебным планом предусмотрены лекционные занятия (40 час.), практические занятия (158 час.), самостоятельная работа студентов (126 час.), контроль (108 час.). Дисциплина реализуется со 2 по 5 курсы в 4-9 семестрах. Форма контроля по дисциплине: в 4, 7-9 семестрах экзамен, 5-6 семестрах зачет.

Дисциплина «Военная подготовка» логически и содержательно связана с такими курсами, как «Безопасность жизнедеятельности», «Политология», «Правоведение», «Физика».

Цель: дать обучающимся знания, навыки и умения, необходимые им для дальнейшего успешного обучения в высших учебных заведениях, преимущественно Министерства обороны Российской Федерации;

Задача:

- формирование мотивации воспитанников к выбору военной специальности и как следствие базовых и профильных учебных предметов на этапе профильного обучения;
- обучение адекватному оцениванию требований будущей профессии и личностных качеств офицера, сопоставлению их со своими способностями, интересами, наклонностями.
- привить кадетам волевые, командирские и методические качества, позволяющие в последующем выполнять обязанности младших командиров курсантских подразделений
- повышение компетентности кадет в выполнении задач военно-профессиональной деятельности по их предназначению;

- увеличение уровня практической подготовки кадет.

Для успешного изучения дисциплины «Военная подготовка» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- способность анализировать физические явления и процессы при решении профессиональных задач (ОПК-1);
- способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-6).

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетентности	
ПК-1 - способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	Знает	основные нормативные правовые акты в области информационной безопасности и защиты информации
	Умеет	использовать программные и аппаратные средства персонального компьютера; пользоваться нормативными документами по защите информации
	Владеет	навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями; навыками работы с нормативно правовыми актами по технической защите информации

Для формирования вышеуказанных компетенций в рамках дисциплины «Военная подготовка» применяются следующие методы обучения: чтение лекций. Используемые оценочные средства: конспект (ПР-7).

Аннотация к рабочей программе дисциплины «Управление рисками»

Курс учебной дисциплины «Управление рисками» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин факультатива учебного плана ФТД.2.

Общая трудоемкость дисциплины составляет 36 часов (1 з.е.). Учебным планом предусмотрены лекции (12 часов), практические занятия (12 часов) и самостоятельная работа студента (12 часов). Дисциплина реализуется на 5 курсе в 10 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Управление рисками» логически и содержательно связана с таким курсом, как «Основы управленческой деятельности».

Содержание дисциплины охватывает следующий круг вопросов: основные составляющие процесса управления проектными рисками; классификацию проектных рисков; организация управления проектными рисками в компаниях; построение реестра и карты проектных рисков; определение толерантности к риску; методы качественного анализа проектных рисков; количественные меры риска, принципы и методы управления рисками проектов; оценка и управление инновационными рисками на основе построения и исследования сетевых моделей бизнес-процессов инновационных проектов, использование аппарата имитационного моделирования; классификация рыночных и финансовых рисков.

Цель изучения дисциплины «Управление рисками» заключается в обеспечении фундаментальной и практической профессиональной подготовки, в области теории и практики управления рисками, а также освоении методов оценки результативности системы управления рисками.

Задачи:

- дать представление о роли финансовых и коммерческих рисков в предпринимательской деятельности;
- охарактеризовать основные виды рисков;

- отразить методы оценки финансовых рисков;
- ознакомить с концепцией минимизации рисков в процессе финансовой деятельности.

Для успешного изучения дисциплины «Управление рисками» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность работать в коллективе, толерантно воспринимать социальные, культурные и иные различия (ОК-6);
- способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-13).

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные и профессиональные компетенции (элементы компетенций).

Код и формулировка компетентности	Этапы формирования компетентности	
ПК-4 – способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знает	концептуально-теоретические основы управления рисками
	Умеет	использовать методы и инструменты управления рисками для принятия управленческих решений по реализации конкретных проектов; применять приемы риск-менеджмента в целях внедрения технологических продуктов и инноваций
	Владеет	навыками анализа и разработки системы риск-менеджмента; навыками разработки систем управления рисками организации, оценки результативности системы управления рисками

Для формирования вышеуказанных компетенций в рамках дисциплины «Управление рисками» применяются следующие методы обучения: чтение лекций с использованием мультимедийного оборудования (проектор), собеседование по итогам выполнения практических заданий. Используемые оценочные средства: собеседование (ОУ-1), конспект (ПР-7).