ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

Институт приоритетных технологий

Кафедра информационной безопасности

ПРОГРАММА ПРАКТИКИ
Учебная практика, экспериментально-исследовательская

Уровень ОПОП: Специалитет
Специальность: 10.05.01 Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)
Форма обучения: Очная
Срок обучения: 2024 - 2030 уч. г.
Способ проведения: Стационарная

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.01 Компьютерная безопасность (приказ № 1459 от 26.11.2020 г.) и учебного плана, утвержденного Ученым советом (от 26.05.2023 г., протокол №9)

Разработчики:
Какорина О. А., кандидат физико-математических наук, заведующий кафедрой

Программа рассмотрена и утверждена на заседании кафедры, протокол № 08 от 30.08.2024 года

Зав. кафедрой  Какорина О. А.

1. Пояснительная записка

Цель практики - подготовка системно и широко мыслящего интеллектуала, владеющего основами теории науки и творческой деятельности, имеющего практические навыки сбора, обработки и анализа данных, результатов научных экспериментов; получение опыта самостоятельной научно-исследовательской деятельности. Научно-исследовательская работа студентов также направлена на достижение следующих целей:

- формирование навыков творческого профессионального мышления путем овладения научными методами познания и исследования;
- обеспечение единства образовательного (учебного и воспитательного), научного и практического процессов;
- создание и развитие условий, обеспечивающих возможность для каждого студента реализовывать свое право на творческое развитие личности и участие в научных исследованиях (в соответствии с его потребностями и способностями);
- подготовка студента к самостоятельным исследованиям, основные результаты которого (как правило) включаются в выпускную квалификационную работу;
- подготовка студента к проведению научных исследований в составе творческого коллектива;
- формирование у студентов компетенций, направленных на приобретение навыков планирования и организации научного исследования и умений выполнения НИР с применением различного оборудования и компьютерных технологий.

Задачи практики:

- формирование навыков творческого профессионального мышления путем овладения научными методами познания и исследования;

- приобрести навыков работы с оборудованием для физических экспериментов;

- приобрести опыт самостоятельной профессиональной деятельности;

- совершенствование навыков сбора, систематизации и анализа информации, необходимой для решения задач в сфере физических исследований;

- сбор, систематизация, обобщение материала, который может быть впоследствии может быть использован для выполнения научно-исследовательской работы.

Программа учебной практики разработана на основании базового учебного плана и рабочих программ дисциплин, базовых для данного вида практики, в соответствии с требованиями ФГОС ВПО.

Учебная практика носит характер ознакомительной деятельности по получению первичных профессиональных умений и навыков в соответствии с профилем подготовки и проводится на учебно-лабораторной базе ВолГУ. Организация учебной практики на всех этапах должна быть направлена на обеспечение непрерывности и последовательности овладения студентами будущей профессией в соответствии с требованиями к уровню подготовки выпускника.

2. Место практики в структуре ОПОП ВО

«Учебная практика, экспериментально-исследовательская» является обязательным видом учебной работы, относится к обязательной части учебного плана ФГОС ВО по специальности 10.05.01 Компьютерная безопасность.

«Учебная практика, экспериментально-исследовательская» проводится на 4 курсе.

Общая трудоемкость учебной практики составляет 2 зачетных единиц(-ы) продолжительностью 72 часов.

Практике «Учебная практика, экспериментально-исследовательская» предшествует изучение дисциплин (практик):

- Администрирование в операционных системах;

- Методы дискретной математики в криптологии;
- Технологии и методы программирования;
- Системы управления базами данных;
- Компьютерные сети.

Учебная практика является логическим завершением изучения данных дисциплин.

Практика проводится без отрыва от аудиторных занятий.

Освоение практики «Учебная практика, экспериментально-исследовательская» является необходимой основой для последующего изучения дисциплин (практик):
- Надежность программных средств;
- Информационная безопасность распределенных информационных систем.

3. Требования к результатам освоения практики

Процесс освоения практики направлен на формирование компетенций.

Выпускник должен обладать следующими общепрофессиональными компетенциями (ОПК):

- ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности.

Студент должен уметь:

использовать средства криптографической и технической защиты информации для решения задач профессиональной деятельности..

Студент должен владеть навыками:

навыками и методиками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности.

- ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем.

Студент должен уметь:

формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем.

Студент должен владеть навыками:

навыками настройки политики безопасности основных операционных систем и локальных компьютерных сетей, построенных на базе основных операционных систем.

- ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

принципы построения современных операционных систем и особенности их применения.

Студент должен уметь:

разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом,

управляемым сообщениями; применять основные методы программирования в выбранной операционной сред.

Студент должен владеть навыками:

навыками системного программирования.

- ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; основы физической защиты объектов информатизации; общие принципы построения и использования современных языков программирования высокого уровня; язык программирования высокого уровня (объектно-ориентированное программирование); язык ассемблера персонального компьютера; современные технологии программирования; показатели качества программного обеспечения; базовые структуры данных; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки вычислительной сложности.

Студент должен уметь:

формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем; пользоваться нормативными документами в области технической защиты информации; анализировать и оценивать угрозы информационной безопасности объекта; формализовать поставленную задачу; работать с интегрированными средами разработки программного обеспечения; разрабатывать эффективные алгоритмы и программы; проводить оценку вычислительной сложности алгоритма; планировать разработку сложного программного обеспечения.

Студент должен владеть навыками:

навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей эффективности технической защиты информации; навыками разработки, отладки, документирования и тестирования программ; навыками использования инструментальных средств отладки и дизассемблирования программного кода; методами оценки качества готового программного обеспечения; навыками разработки алгоритмов для решения типовых профессиональных задач.

- ОПК-14 Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

характеристики и типы систем баз данных; основные языки запросов; физическую организацию баз данных и принципы (основы) их защиты; общие и специфические угрозы безопасности баз данных; основные критерии защищенности баз данных и методы оценивания механизмов защиты; механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных; особенности применения криптографической защиты в системах управления базами данных; этапы проектирования системы защиты в системах управления базами данных.

Студент должен уметь:

проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных; настраивать и применять современные системы управления базами данных; пользоваться средствами защиты, предоставляемыми системами управления базами данных; создавать дополнительные средства защиты баз данных; умеет проводить анализ и оценивание механизмов защиты баз данных.

Студент должен владеть навыками:

методикой и навыками составления запросов для поиска информации в базах данных; методикой и навыками использования средств защиты, предоставляемых системами управления базами данных.

- ОПК-15 Способен администрировать компьютерные сети и контролировать корректность их функционирования

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

архитектуру основных типов современных компьютерных систем; принципы построения современных операционных систем и особенности их применения; основы организации и построения компьютерных сетей; эталонную модель взаимодействия открытых систем; функции, принципы действия и алгоритмы работы сетевого оборудования.

Студент должен уметь:

реализовывать приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах; осуществлять проектирование и оптимизацию функционирования компьютерных сетей.

Студент должен владеть навыками:

администрирования компьютерных сетей; навыками работы с сетевым оборудованием и сетевым программным обеспечением.

- ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений.

Студент должен уметь:

формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

Студент должен владеть навыками:

настройки межсетевых экранов; владеет методиками анализа сетевого трафика.

- ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

основные понятия и методы математического анализа, аналитической геометрии, линейной и векторной алгебры.

Студент должен уметь:

разрабатывать и использовать математические методы в технических приложениях; строить вероятностные модели для конкретных процессов, проводить необходимые расчеты в рамках построенной модели..

Студент должен владеть навыками:

соответствующим математическим аппаратом для решения профессиональных задач.

- ОПК-4.1 Способен организовывать защиту информации в компьютерных системах и сетях (по областям применения)

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

систему нормативных правовых актов и стандартов в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем.

Студент должен уметь:

разрабатывать модели угроз и модели нарушителя компьютерных систем и сетей; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.

Студент должен владеть навыками:

способностью при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

- ОПК-4.2 Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения)

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

принципы построения компьютерных сетей; стек сетевых протоколов операционных систем; виды политик управления доступом и информационными потоками в компьютерных сетях; источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению; методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации; требования по составу и характеристикам подсистем защиты информации применительно к операционным системам.

Студент должен уметь:

оценивать угрозы безопасности информации в компьютерных сетях; производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях; проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах; производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах; оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах.

Студент должен владеть навыками:

управлением средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями; управлением функционирования программно-аппаратных средств защиты информации в компьютерных сетях; контролем над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение; контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах.

- ОПК-4.3 Способен разрабатывать и анализировать корректность политики информационной безопасности компьютерных систем и сетей (по областям применения)

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

последовательность и содержание этапов построения компьютерных сетей; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации; типовые структуры и принципы организации компьютерных сетей; примеры реализации современных локальных и глобальных компьютерных сетей; основные телекоммуникационные протоколы; перспективы развития компьютерных сетей.

Студент должен уметь:

анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем.

Студент должен владеть навыками:

навыками разработки технических заданий на создание средств защиты информации; в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.

- ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспертному контролю

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя объекта информатизации.

Студент должен уметь:

разрабатывать модели угроз и модели нарушителя объекта информатизации; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации.

Студент должен владеть навыками:

навыками разработки проектов нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

- ОПК-7 Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

Алгоритмические основы программирования на языках высокого и низкого уровня; языки программирования высокого и низкого уровня; методы, реализуемые в современных инструментальных средствах программирования.

Студент должен уметь:

осуществлять обоснованный выбор способов организации программ и инструментария программирования при решении профессиональных задач.

Студент должен владеть навыками:

разработки алгоритмов для последующего создания программ на языках общего назначения; навыками использования типовых инструментальных средств программирования для решения профессиональных задач.

- ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

методологию научного исследования для определения параметров и характеристик средств защиты информации.

Студент должен уметь:

применять исследовательский подход в процессе сертификации средств защиты информации.

Студент должен владеть навыками:

навыком и практическим опытом проведения научного исследования в процессе сертификации средств защиты информации.

- ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

Знания, умения, навыки, формируемые по компетенции в рамках практики

Студент должен знать:

основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных; общие и специфические угрозы безопасности операционных систем и систем управления баз данных; основные задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.

Студент должен уметь:

решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.

Студент должен владеть навыками:

решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий.

4. Содержание и технология организации практики

Программой практики предусматривается 72 часа(-ов). За период практики студенты обязаны выполнить следующий объем работ:

№	Этап практики	Содержание этапа	Формируемые компетенции	Количество часов	Оценочные средства для текущего контроля	Количество балл

						ов
Седьмой семестр						
1	Подготовительный	Решение организационных вопросов; установочная конференция; знакомство с задачами и программой практики, требованиями к оформлению отчетной документации; знакомство с объектами и особенностями предстоящей деятельности; инструкция по технике безопасности.	ОПК-10, ОПК-11, ОПК-12, ОПК-13, ОПК-14, ОПК-15, ОПК-16, ОПК-3, ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПК-6, ОПК-7, ОПК-8, ОПК-9	8	собеседование	10
2	Ориентировочный	знакомство с базовой организацией практики; изучение и анализ / обзор нормативно-правовой документации; знакомство с методами работы; изучение / обзор литературы; знакомство с методами исследования.	ОПК-10, ОПК-11, ОПК-12, ОПК-13, ОПК-14, ОПК-15, ОПК-16, ОПК-3, ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПК-6, ОПК-7, ОПК-8, ОПК-9	10	собеседование; письменный отчет (часть)	10
4	Заключительный	подготовка отчета о прохождении практики; подготовка и выступление с докладом-презентацией: итоговая конференция. Зачет.	ОПК-10, ОПК-11, ОПК-12, ОПК-13, ОПК-14, ОПК-15, ОПК-16, ОПК-3, ОПК-4.1, ОПК-4.2, ОПК-4.3,	10	письменный отчет (оформление); отчет о результатах НИР; представление / защита результатов практики	10

			ОПК-6, ОПК-7, ОПК-8, ОПК-9			

5. Отчетная документация по практике

Период контроля: Седьмой семестр

- отчет о прохождении практики;
- отчет о прохождении практики

6. Фонд оценочных средств. Оценочные материалы

6.1. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках освоения практики студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий.

Базовый уровень:

обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий.

Пороговый уровень:

обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне.

Уровень ниже порогового:

система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности.

Шкалы и критерии оценки студентов по практике

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации		Шкала оценивания по БРС
	Экзамен (зачет с оценкой)	Зачет	
Повышенный	5 (отлично)	зачтено	91 и более
Базовый	4 (хорошо	зачтено	71 –90
Пороговый	3 (удовлетворительно)	зачтено	60 – 70
Ниже порогового	2 (неудовлетворительно)	не зачтено	Ниже 60

Критерии оценки по результатам освоения практики

Оценка	Показатели
Отлично	Достигнуты цель и основные задачи практики. Обучающийся демонстрирует высокий уровень умений и навыков практического выполнения задач практики. Обучающийся не испытывает трудности в анализе профессиональной деятельности, умеет самостоятельно проектировать и организовывать собственную деятельность. Отчетная документация о прохождении практики оформлена аккуратно, грамотно, в полном объеме; задание выполнено самостоятельно.
Хорошо	Достигнуты цель и основные задачи практики. Обучающийся

	демонстрирует необходимый уровень умений и навыков практического выполнения задач практики. Обучающийся не всегда может самостоятельно организовать собственную деятельность для решения поставленных перед ним задач. Отчетная документация о прохождении практики оформлена в полном объеме с незначительными замечаниями.
Удовлетворительно	Объем практики выполнен полностью. Обучающийся демонстрирует поверхностные теоретические представления в области будущей профессиональной деятельности. Практические умения и навыки сформированы на репродуктивном уровне. Обучающийся проявляет несамостоятельность в организации собственной деятельности для решения задач практики. Отчетная документация о прохождении практики оформлена с замечаниями.
Неудовлетворительно	Цель и задачи практики не достигнуты. Обучающийся имеет значительные недоработки и замечания по выполнению задания практики.

6.2. Типовые задания по практике

В целях освоения компетенций программы практики предусмотрены следующие вопросы, задания текущего контроля:

- ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности

Студент должен знать:

основные понятия и методы математического анализа, аналитической геометрии, линейной и векторной алгебры

Вопросы, задания:

1. Функция. Свойства функции.

2. Неопределенных интеграл. Свойства. Таблица основных интегралов.

Студент должен уметь:

разрабатывать и использовать математические методы в технических приложениях; строить вероятностные модели для конкретных процессов, проводить необходимые расчеты в рамках построенной модели.

Задания:

1. Описать основные принципы полноты множества R.

2. Описать лемму о конечном покрытии.

Студент должен владеть навыками:

соответствующим математическим аппаратом для решения профессиональных задач

Задания:

1. Вывести предел числовой последовательности.

2. Вывести доказательство теоремы критерия Коши.

- ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспертному контролю

Студент должен знать:

систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя объекта информатизации

Вопросы, задания:

1. Постановление Правительства РФ от 15.04.1995 № 333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны".

2. Постановление Правительства РФ от 03.03.2012 № 171 "Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации".

Студент должен уметь:

разрабатывать модели угроз и модели нарушителя объекта информатизации; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации

Задания:

1. Разработать Инструкцию администратора безопасности информационной системы персональных данных.

2. Разработать модель нарушителя.

Студент должен владеть навыками:

навыками разработки проектов нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации

Задания:

1. Составить документ Описание технологического процесса обработки информации в автоматизированной системе.

2. Подготовить Акт классификации автоматизированной системы.

- ОПК-7 Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ

Студент должен знать:

Алгоритмические основы программирования на языках высокого и низкого уровня; языки программирования высокого и низкого уровня; методы, реализуемые в современных инструментальных средствах программирования

Вопросы, задания:

1. Подготовить Акт классификации автоматизированной системы.

2. Архитектура программного обеспечения.

Студент должен уметь:
осуществлять обоснованный выбор способов организации программ и инструментария программирования при решении профессиональных задач

Задания:
1. Разработка клиентских приложений для работы с документами.

2. Разработка Web - браузера.

Студент должен владеть навыками:
разработки алгоритмов для последующего создания программ на языках общего назначения; навыками использования типовых инструментальных средств программирования для решения профессиональных задач

Задания:
1. Работа с журналами событий в ОС.

2. Построение графиков и диаграмм средствами VS.NET.

- ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей
Студент должен знать:
методологию научного исследования для определения параметров и характеристик средств защиты информации

Вопросы, задания:
1. Какие функции безопасности должны быть реализованы в системе обнаружения вторжений?

2. Функциональные требования и требования доверия, которым должно удовлетворять средство антивирусной защиты.

Студент должен уметь:
применять исследовательский подход в процессе сертификации средств защиты информации

Задания:
1. Правовое обоснование сертификации средств защиты информации.

Студент должен владеть навыками:
навыком и практическим опытом проведения научного исследования в процессе сертификации средств защиты информации

Задания:
1. Составить план процесса сертификации согласно основным этапом сертификации.

- ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации
Студент должен знать:
основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных; общие и специфические угрозы безопасности операционных систем и систем управления баз данных; основные задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Вопросы, задания:

1. Перечислите и поясните основные принципы построения операционных систем.

2. Изложите основные архитектурные особенности ОС UNIX.

Студент должен уметь:

решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Задания:

1. Описать задачи возлагаемые на интерфейс прикладного программирования (API).

2. Осуществить в UNIX запуск новой задачи.

Студент должен владеть навыками:

решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий

Задания:

1. Управлять разрешениями для файлов и папок операционных систем.

2. Сконфигурировать учетные записи пользователей с помощью различных средств операционных систем.

- ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Студент должен знать:

основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

Вопросы, задания:

1. Основные виды уязвимостей криптографических протоколов.

2. Атаки на криптографические протоколы, защитные меры.

Студент должен уметь:

использовать средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

Задания:

1. Схемы разделения секрета. Примеры схем предварительного распределения ключей между n абонентами.

2. Протоколы с нулевым разглашением. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы.

Студент должен владеть навыками:

навыками и методиками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

Задания:

1. Протокол распределения ключей Диффи-Хеллмана.

2. Использования гистограмм при определении вида закона распределения

- ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации

Студент должен знать:

средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем

Вопросы, задания:

1. Политики безопасности операционных систем.

2. Стандарты безопасности операционных систем.

Студент должен уметь:

формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем

Задания:

1. Настроить локальную политику назначения прав пользователей.

2. Разработать политику безопасности ОС в соответствии с заданными требованиями по защите информации.

Студент должен владеть навыками:

навыками настройки политики безопасности основных операционных систем и локальных компьютерных сетей, построенных на базе основных операционных систем

Задания:

1. Настроить политики аудита безопасности ОС.

2. Настроить политики учетных записей.

- ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения

Студент должен знать:

принципы построения современных операционных систем и особенности их применения

Вопросы, задания:

1. Основные понятия, функции, состав и принципы работы операционных систем.

2. Типы ОС, функции и способы использования интерфейса ОС, программный интерфейс, виды интерфейсов.

Студент должен уметь:

разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями; применять основные методы программирования в выбранной операционной сред

Задания:

1. Описать структуру оперативной памяти.

2. Описать различие в архитектурах современных ОС.

Студент должен владеть навыками:
навыками системного программирования

Задания:

1. Построить архитектуру UNIX.

2. Описать сходства и различия файловых систем.

- ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности

Студент должен знать:
средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; основы физической защиты объектов информатизации; общие принципы построения и использования современных языков программирования высокого уровня; язык программирования высокого уровня (объектно-ориентированное программирование); язык ассемблера персонального компьютера; современные технологии программирования; показатели качества программного обеспечения; базовые структуры данных; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки вычислительной сложности

Вопросы, задания:

1. Разработка программного обеспечения. Разработка технического задания.

2. Проектирование и разработка прикладного программного обеспечения.

Студент должен уметь:
формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем; пользоваться нормативными документами в области технической защиты информации; анализировать и оценивать угрозы информационной безопасности объекта; формализовать поставленную задачу; работать с интегрированными средами разработки программного обеспечения; разрабатывать эффективные алгоритмы и программы; проводить оценку вычислительной сложности алгоритма; планировать разработку сложного программного обеспечения

Задания:

1. Обоснование экономической эффективности разрабатываемого программного продукта.

2. Тестирование программного обеспечения.

Студент должен владеть навыками:
навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей эффективности технической защиты информации; навыками разработки, отладки, документирования и тестирования программ; навыками использования инструментальных средств отладки и дизассемблирования программного кода; методами оценки качества готового программного обеспечения; навыками разработки алгоритмов для решения типовых профессиональных задач

Задания:

1. Тестирование программ с помощью специализированных инструментальных средств.

2. Структурное программирование.

- ОПК-14 Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации

Студент должен знать:

характеристики и типы систем баз данных; основные языки запросов; физическую организацию баз данных и принципы (основы) их защиты; общие и специфические угрозы безопасности баз данных; основные критерии защищенности баз данных и методы оценивания механизмов защиты; механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных; особенности применения криптографической защиты в системах управления базами данных; этапы проектирования системы защиты в системах управления базами данных

Вопросы, задания:

1. Приведите примеры СУБД, реализующих реляционную модель БД.

2. Приведите примеры СУБД, сертифицированных ФСТЭК.

Студент должен уметь:

проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных; настраивать и применять современные системы управления базами данных; пользоваться средствами защиты, предоставляемыми системами управления базами данных; создавать дополнительные средства защиты баз данных; умеет проводить анализ и оценивание механизмов защиты баз данных

Задания:

1. Спроектируйте БД в соответствии с требованиями по защите информации.

2. Перечислите компоненты БД.

Студент должен владеть навыками:

методикой и навыками составления запросов для поиска информации в базах данных; методикой и навыками использования средств защиты, предоставляемых системами управления базами данных

Задания:

1. Создайте БД в соответствии с требованиями по защите информации.

2. Создайте пользователя базы данных.

- ОПК-15 Способен администрировать компьютерные сети и контролировать корректность их функционирования

Студент должен знать:

архитектуру основных типов современных компьютерных систем; принципы построения современных операционных систем и особенности их применения; основы организации и построения компьютерных сетей; эталонную модель взаимодействия открытых систем; функции, принципы действия и алгоритмы работы сетевого оборудования

Вопросы, задания:

1. Модель СПС.

2. Информативность источников сообщений. Избыточность источников.

Студент должен уметь:
реализовывать приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах; осуществлять проектирование и оптимизацию функционирования компьютерных сетей

Задания:

1. Перечислите характеристики линий радиосвязи.

2. Перечислите характеристики работы спутниковых ретрансляторов.

Студент должен владеть навыками:
администрирования компьютерных сетей; навыками работы с сетевым оборудованием и сетевым программным обеспечением

Задания:

1. Сконфигурировать имена маршрутизаторов (R-A, R-B) и адреса Fast Ethernet интерфейсов маршрутизаторов.

2. Сконфигурировать последовательные (serial) интерфейсы.

- ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях

Студент должен знать:
средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений

Вопросы, задания:

1. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации.

2. Удалённое определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP.

Студент должен уметь:
формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

Задания:

1. Методы обнаружения пакетных сниферов.

2. Методы обхода МЭ.

Студент должен владеть навыками:
настройки межсетевых экранов; владеет методиками анализа сетевого трафика

Задания:

1. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.

2. Основные возможности и схемы развертывания МЭ.

- ОПК-4.1 Способен организовывать защиту информации в компьютерных системах и сетях (по областям применения)

Студент должен знать:
систему нормативных правовых актов и стандартов в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем

Вопросы, задания:

1. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации.

2. Правовой режим защиты государственной тайны. Закон РФ от 21 июля 1993 г. N 5485-I "О государственной тайне".

Студент должен уметь:
разрабатывать модели угроз и модели нарушителя компьютерных систем и сетей; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы

Задания:

1. Виды конфиденциальной информации и их правовые режимы.

2. Законодательство о техническом регулировании в РФ. Технические регламенты и стандарты. Цели их создания и принципы.

Студент должен владеть навыками:
способностью при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Задания:

1. Разработать разрешительную систему доступа к информационным ресурсам автоматизированной системы.

2. Разработать Положение по обращению со съемными машинными носителями конфиденциальной информации.

- ОПК-4.2 Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения)

Студент должен знать:
принципы построения компьютерных сетей; стек сетевых протоколов операционных систем; виды политик управления доступом и информационными потоками в компьютерных сетях; источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению; методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации; требования по составу и характеристикам подсистем защиты информации применительно к операционным системам

Вопросы, задания:

1. Основные понятия, функции, состав и принципы работы операционных систем.

2. Типы ОС, функции и способы использования интерфейса ОС, программный интерфейс, виды интерфейсов.

Студент должен уметь:
оценивать угрозы безопасности информации в компьютерных сетях; производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях; проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах; производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах; оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

Задания:
1. Описать структуру оперативной памяти.

2. Описать различие в архитектурах современных ОС.

Студент должен владеть навыками:
управлением средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями; управлением функционирования программно-аппаратных средств защиты информации в компьютерных сетях; контролем над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение; контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах

Задания:
1. Построить архитектуру UNIX.

2. Описать логическую организацию файловой системы.

- ОПК-4.3 Способен разрабатывать и анализировать корректность политики информационной безопасности компьютерных систем и сетей (по областям применения)
Студент должен знать:
последовательность и содержание этапов построения компьютерных сетей; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации; типовые структуры и принципы организации компьютерных сетей; примеры реализации современных локальных и глобальных компьютерных сетей; основные телекоммуникационные протоколы; перспективы развития компьютерных сетей

Вопросы, задания:
1. Этапы разработки и функционирования СУИБ.

2. Виртуальные частные сети и наиболее часто используемые протоколы VPN.

Студент должен уметь:
анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем

Задания:

1. Обеспечение защиты информационных ресурсов компании от сетевых атак.

2. Сетевые сканеры уязвимостей, как средства анализа защищенности сетей.

Студент должен владеть навыками:
навыками разработки технических заданий на создание средств защиты информации; в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

Задания:

1. Принципы управления информационной безопасностью.

2. Разработать политику информационной безопасности предприятия.

6.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Оценка качества освоения практики включает текущий контроль успеваемости и промежуточную аттестацию обучающихся.

К основным формам текущего контроля относятся устный опрос, собеседование, письменные задания (формирование письменного отчета). К основным формам промежуточной аттестации относится письменный отчет о прохождении практики.

Устный опрос, собеседование представляет собой средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с целью, задачами практики, техникой безопасности (в случаях прохождения практики на предприятиях или в случаях проведения практики выездным или полевым способом), и рассчитанное на выяснение объема теоретических знаний и умений, необходимых для выполнения заданий в рамках практики. Письменные задания (формирование разделов отчета) – это продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов решения практикоориентированных задач из области будущей профессиональной деятельности; анализа нормативно-правовых документов и др. К основным формам промежуточной аттестации обучающихся является зачет с оценкой. Оценочным средством промежуточной аттестации по практике является письменный отчет обучающегося о прохождении практики. Отчет о прохождении практики оформляются по установленному образцу, включает в себя сведения о месте, сроках прохождения практики, описание выполненных работ в соответствии с этапами практики; отчет содержит отзыв руководителя практики от университета и отзыв руководителя практики от базы практики.

7. Учебно-методическое обеспечение

7.1 Основная литература

1. Баранова Елена Константиновна Информационная безопасность и защита информации [Электронный ресурс]: учебное - Издание 3 - РИОР, 2017. - 322 с. - Режим доступа: http://new.znanium.com/go.php?id=763644

2. Гришина Наталия Васильевна Информационная безопасность предприятия [Электронный ресурс]: учебное - Издание доп. - ФОРУМ, 2017. - 239 с. - Режим доступа: http://new.znanium.com/go.php?id=612572

7.2 Дополнительная литература

1. Шаньгин Владимир Федорович Информационная безопасность компьютерных систем и

сетей [Электронный ресурс]: учебное - ФОРУМ, 2017. - 416 с. - Режим доступа: http://new.znanium.com/go.php?id=775200

В качестве учебно-методического обеспечения могут быть использованы другие учебные, учебно-методические и научные источники по профилю практики, содержащиеся в электронно-библиотечных системах, указанных в п. 7.5 «Электронно-библиотечные системы».

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://elibrary.ru - Научная электронная библиотека

2. http://new.volsu.ru/umnik - Образовательный портал Волгоградского государственного университета «УМНИК»

3. https://e.lanbook.com/ - ЭБС "Лань"

4. https://www.book.ru/ - ЭБС BOOK.ru

7.4. Электронно-библиотечные системы

8. Перечень информационных технологий

В учебном процессе активно используются информационные технологии с применением современных средств телекоммуникации; электронные учебники и обучающие компьютерные программы. Каждый обучающийся обеспечен неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) университета. ЭИОС предоставляет открытый доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к электронным библиотечным системам и электронным образовательным ресурсам.

8.1 Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

Программное обеспечение:
1. Microsoft Windows 7 Professional, 11 лицензий, номер 60357707
2. Microsoft Windows 7 Home Premium, 1 лицензия, OEM-лицензия
3. Microsoft Windows 8.1 Home, 1 лицензия OEM-лицензия
4. Microsoft Office 2007 Standart, 1 лицензия, номер 43847745
5. Microsoft Office 2016, 14 лицензия, Сублицензионный договор No 31604241628 от 21.11.16
6. LibreOffice 12 лицензий (свободно-распространяемое программное обеспечение)
7. FreeBSD, 10 лицензий FreeBSD license свободное программное обеспечение
8. Oracle VM VirtualBox, 14 лицензий GNU GPL свободное программное обеспечение
9. Mozila FireFox, 13 лицензий Mozilla Public License 2.0 (MPL) свободное программное обеспечение
10. Visual Studio Community 2017, 13 лицензий, учебное программное обеспечение
11. Python 2.7, 13 лицензий PSFL (свободно-распространяемое программное обеспечение)
12. Windows 10 Профессиональная, 13 лицензий, номер 65946188.
13. 7-zip, 3 лицензии GNU LGPL свободное программное обеспечение
14. Антивирус Kaspersky Endpoint Security, 3 лицензии, номер 500999

8.2 Перечень информационно-справочных систем
(обновление выполняется еженедельно)

1. Гарант Максимум

2. Консультант Плюс

9. Методические указания для лиц с ОВЗ и инвалидов

Практика для обучающихся с ограниченными возможностями здоровья и инвалидов проводится с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

10. Материально-техническое обеспечение

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
Специализированная мебель:
1. Столы – 8 шт.
2. стулья – 16 шт.
3. парта со скамьей – 8 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.
Демонстрационное оборудование:
1. Проектор BenQ MX 505
2. Экран проекционный
3. Доска (магнитная, маркерная)
Рабочие места на базе вычислительной техники (18 шт):
1.Моноблок VPS 5000 (16 шт.);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
Сетевое оборудование:
1. Wi-Fi роутер ASUS RT-N10
2. Концентратор.
3. Комплекс "Сетевое оборудование "Cisco" часть 1

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
Специализированная мебель:
1. компьютерные столы – 13 шт.
2. стулья – 29 шт.
3. парта – 8 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.
Средства вычислительной техники (15 шт):
1. Компьютерный комплекс Option в составе: Системный блок
клавиатура, мышь, монитор (13 шт);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
Сетевое оборудование:
1. Маршрутизатор ASUS WL-520GU.
2. Концентратор.
Демонстрационное оборудование:
1. Доска (магнитная, маркерная)
2. Проектор projector DLP ColorBoost II
3. Экран для проектора Digis

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
Специализированная мебель:
1. столы – 8 шт
2. стулья – 16 шт.
3. учебные места – 16 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.
Демонстрационное оборудование:
1. Доска (магнитная, маркерная)

Учебная аудитория для проведения занятий семинарского типа, лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций.

Специализированная мебель:
1. компьютерные столы – 15 шт.
2. стулья – 15 шт.
3. рабочее место преподавателя (стол и стул) – 1 шт.
5. Доска (магнитная, маркерная)
Рабочие места на базе вычислительной техники (15 шт.):
1. компьютерный к-кс Intel Core i5 6500 + монитор Acer 21.5"
K222HQLCbid + клавиатура SVEN Standard 301, мышь CBR
CM-102 (10 шт.)
2. Компьютерный комплекс Option в составе: Системный блок, клавиатура, мышь, монитор (2 шт)
3. Ноутбук Acer AS5738G;
4. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
5. Ноутбук 15,6” ASUS P53S/P53SJ, Intel Core i5
структурированная кабельная система:
1. ком-кс "Сетевое оборудование "Cisco" ч.2
2. концентратор