МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СЕРВИСА»
(ФГБОУ ВО «ПВГУС»)

Кафедра «Прикладная информатика в экономике»

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА

по дисциплине **«Эксплуатация систем информационной безопасности»**
для студентов направления подготовки 10.03.01 «Информационная безопасность»
направленности (профиля) «Организация и технология защиты информации»

Тольятти 2018 г.

Рабочая учебная программа по дисциплине «Эксплуатация систем информационной безопасности» включена в основную профессиональную образовательную программу направленности (профиля) «Организация и технология защиты информации» направления подготовки 10.03.01 «Информационная безопасность» решением Президиума Ученого совета (Протокол № 4 от 28.06.2018 г.).

Начальник учебно-методического отдела _____ Н.М. Шемендюк

28.06.2018 г.

Рабочая учебная программа по дисциплине «Эксплуатация систем информационной безопасности» разработана в соответствии с Федеральным государственным образовательным стандартом направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Минобрнауки РФ от 1 декабря 2016 г. N 1515.

Составили: Малышева Е.Ю., Бобровский С.М.

Согласовано Директор научной библиотеки _____ В.Н.Еремина

Согласовано Начальник управления информатизации _____ В.В.Обухов

Рабочая программа утверждена на заседании кафедры «Прикладная информатика в экономике» Протокол № 12 от «22» июня 2018г.

И.о. заведующего кафедрой _____ д.э.н., профессор Бердников В.А.
(подпись) (ученая степень, звание, Ф.И.О.)

Согласовано начальник учебно-методического отдела _____ Н.М.Шемендюк

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

–

1.1. Цели освоения дисциплины

Цель освоения дисциплины – дать представление обо всем комплексе задач организации и управления в сфере информационной безопасности;

освещение основных практических подходов, диктуемых современными бизнес-процессами, к проектированию систем информационной безопасности различной степени сложности, в зависимости от характера объекта защиты.

1.2. В соответствии с видами профессиональной деятельности, на которые ориентирована образовательная программа указанного направления подготовки, содержание дисциплины позволит обучающимся решать следующие профессиональные задачи:

эксплуатационная деятельность:

– установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

– администрирование подсистем информационной безопасности объекта;

проектно-технологическая деятельность:

– сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

– проведение проектных расчетов элементов систем обеспечения информационной безопасности;

экспериментально-исследовательская деятельность:

– сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

– проведение экспериментов по заданной методике, обработка и анализ их результатов.

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины у обучающихся формируются следующие компетенции:

Код компетенции	Наименование компетенции
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.
ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

1.4. Перечень планируемых результатов обучения по дисциплине

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
Знает: Структура и содержание политики информационной безопасности; Основные направления реализации политики информационной безопасности (ПК-4);	*Лекции, лекция с разбором конкретных ситуаций, проблемные лекции, практические занятия; самостоятельная работа.*	*Тестирование, собеседование. подготовка докладов.*

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
Структуру и состав исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-7); Принципы построения систем защиты информации (ПК-7); Методы анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)		
Умеет: Разрабатывать политики безопасности информации автоматизированных систем (ПК-4); Планировать политику безопасности программных компонентов автоматизированных систем (ПК-4); Собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-7); Проводить анализ структурных и функциональных схем защищенной автоматизированной системы (ПК-7); Проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)	*Лекции, лекция с разбором конкретных ситуаций, проблемные лекции, практические занятия; самостоятельная работа. написание письменной работы (реферата), выполнение творческого задания.*	*Тестирование, собеседование, доклад по реферату, защита проекта.*
Имеет практический опыт: Формирования политики информационной безопасности в автоматизированных системах (ПК-4); Сбора и и анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-7). анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10).	*лекция с разбором конкретных ситуаций, практические занятия; самостоятельная работа. написание письменной работы (реферата), выполнение творческого задания.*	*Собеседование, доклад по реферату, защита проекта.*

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам по выбору вариативной части дисциплин по направлению подготовки 10.03.01 «Информационная безопасность». Ее освоение осуществляется в 7 семестре (очная форма обучения), 8 семестре (очно-заочная форма обучения).

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Код и наименование компетенций
	Предшествующие дисциплины	
1	«Основы информационной безопасности»	ОК-5, ОПК-7
2	«Аппаратные средства вычислительной техники»	ПК-1, ПК-6
3	«Программно-аппаратные средства защиты информации»	ОПК-7, ПК-6
4	«Техническая защита информации»	ОПК-11, ПСК-1, ПК-15

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Распределение фонда времени по семестрам и видам занятий

Виды занятий	очная форма обучения	очно-заочная форма обучения
Итого часов Зачетных единиц	180 ч. 5 з.е.	180 ч. 5 з.е.
Лекции (час)	32	6
Практические (семинарские) занятия (час)	42	10
Лабораторные работы (час)	-	-
Самостоятельная работа (час)	79	155
Курсовой проект (+,-)	+	+
Контрольная работа (+,-)	-	-
Экзамен, семестр /час.	7 СЕМЕСТР /27 ч.	8 СЕМЕСТР /9 ч.
Зачет (дифференцированный зачет), семестр	-	-
Контрольная работа, семестр	-	-

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость *(в часах)*				Средства и технологии оценки
		Лекции	Практ. Занятия	Лабор. Занятия	Самост. Работа	
1	*Тема 1. Архитектура СИБ. Основные требования к системам ИБ.* Задача проектирования системы ИБ. Построение архитектуры системы ИБ, как интегрированного решения. Эффективность системы ИБ. Интегрированная архитектура систем ИБ. Задачи, которые решаются с помощью компонентов комплексной системы ИБ. Управление компонентами системы ИБ.	4/1	4/1	0/0	10/25	Тестирование, собеседование, доклад по реферату, защита проекта, отчет по практической работе в печатной форме в соответствии с требованиями к оформлению
2	*Тема 2. Основные этапы построения и внедрения*	6/1	8/1	0/0	14/26	Тестирование,

№ п/п	Раздел дисциплины	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость *(в часах)*				Средства и технологии оценки
		Лекции	Практ. Занятия	Лабор. Занятия	Самост. Работа	
	систем информационной безопасности. Работы по созданию и сопровождению СИБ. Работы по созданию и сопровождению подсистемы защиты информации. Этапы: работ по созданию и сопровождению подсистемы защиты информации. Порядок определения требований к защищенности циркулирующей в системе информации. Оценка требований к защищенности некоторого типа информационных пакетов. Наиболее актуальные источники угроз на уровне бизнес-процессов. Формирование требований к проектируемой системе защиты информации.					собеседование, доклад по реферату, защита проекта, отчет по практической работе в печатной форме в соответствии с требованиями к оформлению
3	*Тема 3.. Анализ рисков.* Идентификация методики оценки рисков, удовлетворяющую требованиям конкретной системы информационной безопасности. Критерии принятия рисков и определение допустимых уровней риска. Определение угроз. Оценка влияния угроз и уязвимостей на активы. Принятие надлежащих мер управления безопасностью для уменьшения риска.	4/1	6/2	0/0	14/26	Тестирование, собеседование, доклад по реферату, защита проекта, отчет по практической работе в печатной форме в соответствии с требованиями к оформлению
4	*Тема 4.: Разработка организационных и нормативно-технических документов.* Разработка концепции ИБ. Разработка программы осведомленности позволяет создать механизм информирования всех сотрудников о требованиях по ИБ и поддержку этой информированности на необходимом уровне. Разработка регламентов и документированных процедур по различным аспектам деятельности по защите информации (регламент реагирования на инциденты, резервного копирования и восстановления, антивирусной защиты и др.) и инструкций для персонала. Разработка политики ИБ, фиксирующей детальные требования к различным процессам и техническим средствам, связанным с ИБ.	6/1	8/2	0/0	14/26	Тестирование, собеседование, доклад по реферату, защита проекта, отчет по практической работе в печатной форме в соответствии с требованиями к оформлению
5	*Тема 5.. Политика информационной безопасности организации.* Совокупность технических, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, четко регламентирующих все вопросы обеспечения безопасности информации. Общая характеристика автоматизированных систем организации. Цели и принципы информационной безопасности. Основные направления, способы и требования по обеспечению безопасности информации. Перечень документов, выпускаемых в поддержку политики безопасности.	6/1	8/2	0/0	14/26	Тестирование, собеседование, доклад по реферату, защита проекта, отчет по практической работе в печатной форме в соответствии с требованиями к оформлению
6	Тема 6. Проведение регулярной проверки системы информационной безопасности для определения достаточности принимаемых мер в следующих аспектах: Соответствие системы требованиям стандартов, законодательства или норм. Отвечает ли система	6/1	8/2	0/0	13/26	Тестирование, собеседование, доклад по реферату, защита проекта, отчет по практической работе в печатной форме в соответствии с

№ п/п	Раздел дисциплины	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость *(в часах)*				Средства и технологии оценки
		Лекции	Практ. Занятия	Лабор. Занятия	Самост. Работа	
	определенным требованиям информационной безопасности. Эффективность применяемых мер и поддержка в рабочем состоянии; Выполняется ли меры в том объеме, в котором были запланированы; Результаты внутреннего аудита и анализа системы со стороны руководства.					требованиями к оформлению
		32/6	42/ 10	0/0	79/155	
	Промежуточная аттестация по дисциплине					Экзамен, курсовой проект

Примечание:
-/- объем часов соответственно для очной, очно-заочной форм обучения.

4.2. Содержание практических занятий

№	Наименование темы практических (семинарских) занятий	Обьем часов	Форма проведения
	7 семестр / 8 семестр		
1	Практическая работа 1.. Цель; изучить основные требования к системам ИБ и основным элементам архитектуры СИБ. Задание: 1. По заданным источникам изучить и основным элементам архитектуры СИБ. 1. Для заданной предметной области сформулировать основные требования к системе ИБ. Оформить в виде краткого технического задания. **2.** Определить структуру, состав и основные требования к элементам архитектуры СИБ.	4/1/-	решение разноуровневых и проблемных задач, отчет по практической работе в печатной форме в соответствии с требованиями к оформлению
2	Практическая работа 2. Основные этапы построения и внедрения систем информационной безопасности. Работы по созданию и сопровождению СИБ Цель; изучить основные этапы построения и внедрения систем информационной безопасности. Задание: 1. Для заданной предметной области сформулировать основные этапы построения и внедрения системы информационной безопасности. Этапы работ структурировать в виде процессной модели IDEF0 или DFD. 2. Разработать требования к составу работ и результатам каждого этапа по п.1 задания. 3. Определить основные виды процессов и работ по сопровождению СИБ. Разработать требования к составу работ и результатам каждого вида работ.	8/1/-	решение разноуровневых и проблемных задач, отчет по практической работе в печатной форме в соответствии с требованиями к оформлению
3	Практическая работа 3. Анализ рисков. Цель; изучить основные методики и этапы анализа рисков ИБ. Задание: 1. Для заданной предметной области определить угрозы. Оценить влияние угроз и	6/2/-	решение разноуровневых и проблемных задач, отчет по практической работе в печатной форме в соответствии

№	Наименование темы практических (семинарских) занятий	Обьем часов	Форма проведения
	уязвимостей на активы. 2. Выполнить идентификацию методики оценки рисков, удовлетворяющей требованиям конкретной системы информационной безопасности. 3. Определить критерии принятия рисков и допустимые уровни риска. 4. Разработать систему мероприятий управления безопасностью для уменьшения риска.		с требованиями к оформлению
4	Практическая работа 4. Разработка организационных и нормативно-технических документов. Цель; изучить основные организационные и нормативно-технические документы системы ИБ организации Задание: 1. Для заданной предметной области разработать требования к политике ИБ. 2. Разработать требования к системе политик ИБ, фиксирующих детальные требования к различным процессам и техническим средствам, связанным с ИБ. 3. Разработать *регламенты и документированные процедуры* по различным аспектам деятельности по защите информации (регламент реагирования на инциденты, резервного копирования и восстановления, антивирусной защиты и др.) и *инструкции* для персонала.	8/2/-	решение разноуровневых и проблемных задач, отчет по практической работе в печатной форме в соответствии с требованиями к оформлению
5	Практическая работа 5. Политика информационной безопасности организации Цель; изучить основные требования к составу и содержанию системы Политик информационной безопасности. Задание: 1. Для заданной предметной области разработать политику ИБ. 2. Разработать систему политик ИБ, фиксирующих детальные требования к различным процессам и техническим средствам, связанным с ИБ.	8/2/-	решение разноуровневых и проблемных задач, отчет по практической работе в печатной форме в соответствии с требованиями к оформлению
6	Практическая работа 6. Внутренний аудит системы информационной безопасности. Цель; изучить основные требования к внутреннему аудиту системы информационной безопасности. Задание: 1. Для заданной предметной области разработать программу внутреннего аудита системы ИБ. 2. Оформить результаты внутреннего аудита. 3. Разработать корректирующие мероприятия по результатам внутреннего аудита. 4. Разработать мероприятия по анализу системы ИБ со стороны руководства.	8/2/-	решение разноуровневых и проблемных задач, отчет по практической работе в печатной форме в соответствии с требованиями к оформлению
	Итого	42/10/-	

4.3. Содержание лабораторных работ

Лабораторных работ в учебном плане не предусмотрено

5. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Содержание самостоятельной работы

1. Изучение лекционного материала по конспектам лекций, рекомендуемой литературе, электронным ресурсам.
2. Подготовка к практическим занятиям.
3. Оформление отчетов по результатам практических занятий.
3. Подготовка, написание и оформление курсового проекта.

Контроль самостоятельной работы осуществляется в виде проверки конспектов по самостоятельно изученным вопросам, опросу на лекциях, тестирований, защиты практических работ, результатов выполнения соответствующих учебных упражнений и примеров, контроля подготовки курсового проекта.

Технологическая карта самостоятельной работы студента

Код реализуемой компетенции	Вид деятельности студентов (задания на самостоятельную работу)	Итоговый продукт самостоятельной	Средства и технологии оценки	Обьем часов
ПК-4	- самостоятельное изучение тем дисциплины; подготовка к практическим занятиям; - изучение рекомендуемой литературы, информационно-библиотечных источников, учебно-методических изданий и др.	*конспект, реферрат, отчет по практической работе*	*собеседование, письменная работа*	27/52/-
ПК-7	- самостоятельное изучение тем дисциплины; подготовка к практическим занятиям; - изучение рекомендуемой литературы, информационно-библиотечных источников, учебно-методических изданий и др.	*конспект, реферрат, отчет по практической работе*	*собеседование, письменная работа*	26/52/-
ПК-10	- самостоятельное изучение тем дисциплины; подготовка к практическим занятиям; - изучение рекомендуемой литературы, информационно-библиотечных источников, учебно-методических изданий и др.	*конспект, реферрат, отчет по практической работе*	*собеседование, письменная работа*	26/51/-
				79/155/-

Содержание заданий для самостоятельной работы

№	*Тема*	*Тема самостоятельной работы*
1.	*Тема 1. Архитектура СИБ. Основные требовани к системам ИБ.*	СИБ в современных организациях. Сложная многокомпонентная, многоуровневая, территориально и логически распределенная архитектура. Компоненты ПИБ. Программные и технические средства обеспечения ИБ. Телекоммуникационное и компьютерное оборудование, операционные системы и приложения. Специализированные средства защиты информации, Система организационных мероприятий и ИТ-процессов (процедур) по обеспечению ИБ. Управление инцидентами, цели, задачи, способы. Состав ПИБ: компоненты и подсистемы, интегрированные между собой и с другими компонентами ИТ-инфраструктуры:
2.	*Тема 2. Основные этапы построения и внедрения систем информационной безопасности. Работы по созданию и сопровождению СИБ*	Этапы: работ по созданию и сопровождению подсистемы защиты информации. Предварительное обследование объекта информатизации с целью определения его текущего состояния, выработки требований по обеспечению безопасности, документирование ИС, выдачи рекомендаций (Аудит безопасности). Построение модели нарушителя, обзор методов. Разработка Концепции обеспечения информационной безопасности. Подготовка технического задания на создание. Подсистемы информационной безопасности ИС. Проектирование СИБ (разработка технического проекта). Разработка организационно-распорядительных документов по обеспечению информационной безопасности. Разработка рабочего проекта Сопровождение СИБ, техническая поддержка, аутсорсинг услуг по обеспечению информационной безопасности.
3.	*Тема 3.. Анализ рисков.*	Идентификация методики оценки рисков, удовлетворяющую требованиям конкретной системы информационной безопасности. Критерии принятия рисков и определение допустимых уровней риска. Определение угроз. Оценка влияния угроз и уязвимостей на активы. Принятие надлежащих мер управления безопасностью для уменьшения риска.
4.	*Тема 4.: Разработка организационных и нормативно-технических документов***.**	Разработка концепции ИБ. Разработка программы осведомленности позволяет создать механизм информирования всех сотрудников о требованиях по ИБ и поддержку этой информированности на необходимом уровне. Разработка регламентов и документированных процедур по различным аспектам деятельности по защите информации (регламент реагирования на инциденты, резервного копирования и восстановления, антивирусной защиты и др.) и инструкций для персонала. Разработка политики ИБ, фиксирующей детальные требования к различным процессам и техническим средствам, связанным с ИБ.
5.	*Тема 5.. Политика информационной безопасности организации*	Совокупность технических, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, четко регламентирующих все вопросы обеспечения безопасности информации. Общая характеристика автоматизированных систем организации. Цели и принципы информационной безопасности. Основные направления, способы и требования по обеспечению безопасности информации. Перечень документов, выпускаемых в поддержку политики безопасности.
6.	*Тема 6.. Внутренний аудит системы информационной безопасности*	Проведение регулярной проверки системы информационной безопасности для определения достаточности принимаемых мер в следующих аспектах: Соответствие системы требованиям стандартов, законодательства или норм. Отвечает ли система определенным требованиям информационной безопасности. Эффективность применяемых мер и поддержка в рабочем состоянии; Выполняется ли меры в том объеме, в котором были запланированы;

№	Тема	Тема самостоятельной работы
		Результаты внутреннего аудита и анализа системы со стороны руководства.

Рекомендуемая литература *1, 2, 3, 4, 5, 6, 7.*

6. Методические указания для обучающихся по освоению дисциплины

Инновационные образовательные технологии

Используемые интерактивные образовательные технологии: изучение материалов по презентациям к лекциям, видеоурокам; компьютерное тестирование по результатам освоения разделов изучаемой дисциплины.

№	Вид образовательных технологий, средств передачи знаний, формирования умений и практического опыта	№ темы / тема лекции	№ практической работы / перечень
1.	Лекция-дискуссия, Метод анализа конкретных ситуаций на практических работах.	*Тема 1. Архитектура СИБ. Основные требования к системам ИБ.*	*Практическая работа 1. Архитектура СИБ.*
2.	Лекция-дискуссия, Метод анализа конкретных ситуаций на практических работах.	*Тема 2. Основные этапы построения и внедрения систем информационной безопасности. Работы по созданию и сопровождению СИБ*	*Практическая работа 2.Основные этапы построения и внедрения систем информационной безопасности. Работы по созданию и сопровождению СИБ*
3.	Лекция-дискуссия	*Тема 3.. Анализ рисков.*	*Практическая работа 3. Анализ рисков.*
4.	Лекция-дискуссия	*Тема 4.: Разработка организационных и нормативно-технических документов.*	*Практическая работа 4. Разработка организационных и нормативно-технических документов.*
5	Лекция-дискуссия	*Тема 5.. Политика информационной безопасности организации.*	*Практическая работа 5. Политика информационной безопасности организации:*
6	Лекция-дискуссия, Метод анализа конкретных ситуаций на практических работах.	*Тема 6.. Внутренний аудит системы информационной безопасности.*	*Практическая работа 6. Внутренний аудит системы информационной безопасности.*

Для повышенного уровня - участие в конференции, написание реферата, написание статьи под руководством преподавателя.

- В начале семестра студентам необходимо ознакомиться с технологической картой дисциплины, выяснить, какие результаты освоения дисциплины заявлены (знания, умения, практический опыт). Для успешного освоения дисциплины студентам необходимо выполнить задания, предусмотренные рабочей учебной программой дисциплины и пройти контрольные точки в сроки, указанные в технологической карте (раздел 11). От качества и полноты их выполнения будет зависеть уровень сформированности компетенции и оценка текущей успеваемости по дисциплине. По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной

аттестации, если это предусмотрено технологической картой дисциплины. Списки учебных пособий, научных трудов, которые студентам следует прочесть и законспектировать, темы практических занятий и вопросы к ним, вопросы к экзамену (зачету) и другие необходимые материалы указаны в разработанном для данной дисциплины учебно-методическом комплексе.

- Основной формой освоения дисциплины является контактная работа с преподавателем - лекции, практические занятия, консультации (в том числе индивидуальные), в том числе проводимые с применением дистанционных технологий.
- По дисциплине часть тем (разделов) изучается студентами самостоятельно. Самостоятельная работа предусматривает подготовку к аудиторным занятиям, выполнение заданий (письменных работ, творческих проектов и др.) подготовку к промежуточной аттестации (экзамену (зачету)).
- На лекционных и практических (семинарских) занятиях вырабатываются навыки и умения обучающихся по применению полученных знаний в конкретных ситуациях, связанных с будущей профессиональной деятельностью. По окончании изучения дисциплины проводится промежуточная аттестация (экзамен, (зачет)).
- Регулярное посещение аудиторных занятий не только способствует успешному овладению знаниями, но и помогает организовать время, т.к. все виды учебных занятий распределены в семестре планомерно, с учетом необходимых временных затрат.

6.1. Методические указания для обучающихся по освоению дисциплины на практических занятиях

-
- Практические занятия обучающихся обеспечивают:
- - проверку и уточнение знаний, полученных на лекциях;
- - получение навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;
- - обсуждение вопросов в аудитории, разделенной на группы 6 - 8 обучающихся либо индивидуальных;
- - выполнение практических заданий, задач;
- - подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины;
- - другое.

Содержание заданий для практических занятий

Практическая работа 1..

Цель; изучить основные требования к системам ИБ и основным элементам архитектуры СИБ.

Задание: 1. По заданным источникам изучить и основным элементам архитектуры СИБ.

3. Для заданной предметной области сформулировать основные требования к системе ИБ. Оформить в виде краткого технического задания.

4. Определить структуру, состав и основные требования к элементам архитектуры СИБ.

Практическая работа 2. Основные этапы построения и внедрения систем информационной безопасности. Работы по созданию и сопровождению СИБ Цель; изучить основные этапы построения и внедрения систем информационной безопасности.

Задание: 1. Для заданной предметной области сформулировать основные этапы построения и внедрения системы информационной безопасности. Этапы работ структурировать в виде процессной модели IDEF0 или DFD.

2. Разработать требования к составу работ и результатам каждого этапа по п.1 задания.

3. Определить основные виды процессов и работ по сопровождению СИБ. Разработать требования к составу работ и результатам каждого вида работ.

Практическая работа 3. Анализ рисков.

Цель; изучить основные методики и этапы анализа рисков ИБ.

Задание: 1. Для заданной предметной области определить угрозы. Оценить влияние угроз и уязвимостей на активы.

2. Выполнить идентификацию методики оценки рисков, удовлетворяющей требованиям конкретной системы информационной безопасности.

3. Определить критерии принятия рисков и допустимые уровни риска.

4. Разработать систему мероприятий управления безопасностью для уменьшения риска.

Практическая работа 4. Разработка организационных и нормативно-технических документов.

Цель; изучить основные организационные и нормативно-технические документы системы ИБ организации

Задание: 1. Для заданной предметной области разработать требования к политике ИБ.

2. Разработать требования к системе политик ИБ, фиксирующих детальные требования к различным процессам и техническим средствам, связанным с ИБ.

3. Разработать *регламенты и документированные процедуры* по различным аспектам деятельности по защите информации (регламент реагирования на инциденты, резервного копирования и восстановления, антивирусной защиты и др.) и *инструкции* для персонала.

Практическая работа 5. Политика информационной безопасности организации

Цель; изучить основные требования к составу и содержанию системы Политик информационной безопасности.

Задание: 1. Для заданной предметной области разработать политику ИБ.

2. Разработать систему политик ИБ, фиксирующих детальные требования к различным процессам и техническим средствам, связанным с ИБ.

Практическая работа 6. Внутренний аудит системы информационной безопасности.

Цель; изучить основные требования к внутреннему аудиту системы информационной безопасности.

Задание: 1. Для заданной предметной области разработать программу внутреннего аудита системы ИБ.

2. Оформить результаты внутреннего аудита.

3. Разработать корректирующие мероприятия по результатам внутреннего аудита.

4. Разработать мероприятия по анализу системы ИБ со стороны руководства.

Контрольные вопросы для самопроверки

1. Что понимают под угрозой безопасности данных
2. Дайте определение информационной безопасности
3. Дайте определение методу (способу) защиты данных
4. Перечислите требования к необходимым механизмам защиты информационных систем
5. В чуть заключается суть организационно-экономических мер защиты программных продуктов?
6. Перечислите модули системы технической защиты ПО от несанкционированного использования. Кратко охарактеризуйте функции каждого из них.
7. На какие из модулей системы защиты ПО от несанкционированного использования обычно осуществляет атаку злоумышленник?
8. СИБ в современных организациях. Сложная многокомпонентная, многоуровневая, территориально и логически распределенная архитектура.
9. Архитектура СИБ. Компоненты СИБ.
10. Программные и технические средства обеспечения ИБ.
11. Система организационных мероприятий и ИТ-процессов (процедур) по обеспечению ИБ.
12. Управление инцидентами, цели, задачи, способы.
13. Состав СИБ: компоненты и подсистемы, интегрированные между собой и с другими компонентами ИТ-инфраструктуры:
14. Основные этапы построения и внедрения систем информационной безопасности.
15. Этапы: работ по созданию и сопровождению подсистемы защиты информации.
16. Предварительное обследование объекта информатизации с целью определения его текущего состояния, выработки требований по обеспечению безопасности, документирование ИС.

17. Выдача рекомендаций. Аудит безопасности.
18. Построение модели нарушителя, обзор методов.
19. Разработка Концепции обеспечения информационной безопасности.
20. Подготовка технического задания на создание. Подсистемы информационной безопасности ИС.

21. Разработка организационно-распорядительных документов по обеспечению информационной безопасности.
22. Разработка рабочего проекта
23. Состав критичных информационных ресурсов и основные принципы их защиты.
24. Принципы обеспечения ИБ. Применение определенных методов и технологий защиты.
25. Применение конкретных программно-технических средств защиты и системы организационных мероприятий.
26. Проектирование СИБ. Цель проектирования СИБ.
27. Реализация комплексного подхода к обеспечению ИБ.
28. Разработка технического проекта СИБ на основе согласованного с Заказчиком Технического задания, а также существующей Концепции обеспечения ИБ.
29. Описание основных технических решений по созданию СИБ и организационных мероприятий по подготовке СИБ к вводу в действие;
30. Спецификация на комплекс технических средств СИБ;
31. Спецификация на комплекс программных средств СИБ.
32. Рабочих проект СИБ и его элементы.
33. Программно-техническая документация, инструкции, регламенты и прочие организационно-распорядительные документы по обеспечению ИБ
34. План ввода СИБ в эксплуатацию.
35. Сопровождение СИБ, техническая поддержка, аутсорсинг услуг по обеспечению информационной безопасности.
36. Идентификация методики оценки рисков, удовлетворяющей требованиям конкретной системы информационной безопасности.
37. Критерии принятия рисков и определение допустимых уровней риска.
38. Определение угроз. Оценка влияния угроз и уязвимостей на активы.
39. Принятие надлежащих мер управления безопасностью для уменьшения риска.
40. Разработка концепции ИБ. Разработка программы осведомленности.
41. Разработка регламентов и документированных процедур по различным аспектам деятельности по защите информации (регламент реагирования на инциденты, резервного копирования и восстановления, антивирусной защиты и др.) и инструкций для персонала.
42. Разработка политики ИБ, фиксирующей детальные требования к различным процессам и техническим средствам, связанным с ИБ.
43. Политики безопасности, разрабатываемые на основе Концепции. Создание и внедрение политики безопасности.
44. Общая характеристика автоматизированных систем организации.
45. Цели и принципы информационной безопасности. Основные направления, способы и требования по обеспечению безопасности информации.
46. Перечень документов, выпускаемых в поддержку политики безопасности.
47. Проведение регулярной проверки системы информационной безопасности для определения достаточности принимаемых мер.
48. Соответствие системы требованиям стандартов, законодательства или норм. Отвечает ли система определенным требованиям информационной безопасности.
49. Эффективность применяемых мер и поддержка в рабочем состоянии; Выполняется ли меры в том объеме, в котором были запланированы;
50. Результаты внутреннего аудита и анализа системы со стороны руководства.

Лабораторные работы учебным планом не предусмотрены.

6.2. Методические указания для выполнения контрольных работ

Контрольная работа по дисциплине учебным планом не предусмотрена.

6.3. Методические указания для выполнения курсового проекта

Курсовая работа (проект), рассматриваются как вид учебной работы по дисциплине и выполняются в пределах часов, отводимых на ее изучение. Выполнение курсовых работ (проектов) по дисциплинам осуществляется в соответствии с тематикой, сформированной в соответствии с содержанием дисциплины, сопряженным с направленностью (профилем) образовательной программы. Подготовка курсовой работы (проекта) содействует лучшему усвоению обучающимися учебного материала, формирует практический опыт и умения по изучаемой дисциплине, способствует формированию у обучающихся навыков поиска и критического анализа научной литературы, готовит их к самостоятельной профессиональной деятельности, повышает уровень профессиональной подготовки, является подготовительным этапом к написанию выпускником выпускной квалификационной работы.

Выполнение курсовых работ (проектов) предусматривается по дисциплинам, формирующим последовательно профессиональные компетенции выпускника, и служит основой для выполнения выпускной квалификационной работы.

Курсовой проект по дисциплине «Эксплуатация систем информационной безопасности» по правилам оформления должен соответствовать требованиям к курсовым проектам, утвержденным на кафедре.

Выбор варианта темы курсового проекта и предметной области определяет преподаватель.

Литература [1, 2, 3, 4, 5, 6, 9]

Курсовой проект по дисциплине «Эксплуатация систем информационной безопасности» по правилам оформления должен соответствовать требованиям к курсовым проектам, утвержденным на кафедре.

Курсовой проект позволяет закрепить и углубить знания по дисциплине «Эксплуатация систем информационной безопасности», приобрести навыки использования современных научных достижений в разработке программных и аппаратных средств защиты и безопасности информации и является подтверждением того, что студент умеет применить полученные знания при решении конкретной задачи.

Целью выполнения курсового проекта является приобретение студентами практических навыков в построения систем защиты информации, изучении структуры, основного назначения и характерных особенностей программного и аппаратного обеспечения защиты и безопасности информации в компьютерных системах.

В задачи курсового проекта по дисциплине «Эксплуатация систем информационной безопасности» входит:

- получение знаний в области программного и аппаратного обеспечений защиты и безопасности информации;
- изучение классификации средств, методов защиты информации;
- развитие навыков программирования, полученных на предыдущих курсах;
- развитие системное мышление;
- умение обобщать информацию и делать соответствующие выводы.
- написание программы, соответственно варианту задания.

Последовательность выполнения курсового проекта

- выбрать вариант задания по номеру зачетной книжки.
- провести теоретическое исследование.
- составить аналитическое описание предметной области.
- на основе знаний, полученных в результате исследования и лекционных занятий, разработать проектную часть курсового проекта по защите информации, согласно варианту.
- составить и оформить пояснительную записку по курсовому проекту с описанием всех пунктов согласно задания.

Структура проекта:

Введение. (1–2 стр.), обзор состояния вопроса с характеристикой защищаемого объекта, вариант задания,

1. Аналитическая часть

- Описание предметной области: структура предприятия, основные виды деятельности и процессы, основные объекты инфраструктуры.
- Структура информационной системы предприятия.
- Задачи обеспечения ИБ на предприятии и задачи программно-аппаратной защиты информации на предприятии. Анализ и выявление объектов защиты.
- Анализ и выявление возможных каналов утечки информации и несанкционированного доступа к ресурсам, основных угроз.
- Техническое задание на разработку системы, предложения по повышению уровня защиты (по согласованию с руководителем).

2. Проектная часть.

- Определение каналов утечки информации и несанкционированного доступа к ресурсам с привязкой к объектам.
- Анализ и выбор основных подходов к защите информации на предприятии.
- Определение основных элементов системы ЗИ предприятия.
- Составление плана ЗИ на объекте. Планирование защитных мероприятий по различным направлениям (по объектам, по видам угроз, по видам дестабилизирующего воздействия).
- разработка системы (программного модуля), предложения по повышению уровня защиты.

Заключение.
Библиографический список.
Приложения.

Общий объем курсового проекта — не менее 40–44 страниц.

ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ
по дисциплине «Эксплуатация систем информационной безопасности»

1. Проект мероприятий эксплуатации системы информационной безопасности предприятия _____ .
2. Разработка системы защиты информации предприятия «….».
3. Совершенствование системы защиты информации предприятия «….».
4. Информационная безопасность, как элемент конкурентоспособности организации «…..».
5. Обоснование выбора информационной системы для внедрения на предприятии «…….» с учетом информационной безопасности.
6. Политика информационной безопасности для предприятия «….».
7. Обеспечение защиты данных в информационной системе "….." на предприятии «…….».
8. Системы обнаружения атак. Внедрение программных средств обнаружения атак для информационной системы предприятия «…..».
9. Политика информационной безопасности для системы кадрового агентства.
10. Защита системного и прикладного программного обеспечения ИС на предприятии « ….».
11. Информационная безопасность технологии виртуальных частных сетей.
12. Создание комплексной системы информационной безопасности компьютера, подключенного к локальной сети.

Выбор варианта темы курсового проекта определяет преподаватель. При этом уточняется предметная область проекта и состав проектной части.

Предметная область выбирается по согласованию с преподавателем.

Вариант	Предметная область
1	Завод по сборке автомобилей..
2	Предприятие по выпуску хлебобулочных изделий (хлебозавод) .
3	Предприятие по выпуску комплектующих изделий и узлов для автомобилей.
4	Завод по производству синтетического каучука.
5	Завод по производству минеральных удобрений.
6	Предприятие по выпуску пива и безалкогольных напитков..
7	Предприятие по выпуску мороженого и кондитерских изделий.
8	Книжное издательство.
9	Мебельная фабрика.

Вариант	Предметная область
10	Торговая сеть универмагов (промтовары), работающая под своей торговой маркой
11	Предприятие и торговая сеть по сборке и продаже компьютеров и комплектующих для них.
12	Сеть компьютерных сервисных центров, работающих под своей торговой маркой.
13	Сеть гостиниц (отелей).
14	Банк. Центральный офис и филиалы по работе с клиентами.
15	Страховая компания. Заключение договоров и обслуживание клиентов.
16	Городская телефонная сеть. Учет местных и междугородных переговоров.
17	Сеть оптовых и мелкооптовых складов. Заключение договоров с поставщиками и клиентами, обслуживание клиентов.
18	Торговая фирма (дилерский центр), занимающийся реализацией автомобилей. Работа с клиентами.
19	Сеть ресторанов, работающая под своей торговой маркой. Обслуживание посетителей.
20	Сеть городских библиотек. Выдача книг. Обслуживание посетителей.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (экзамен)

Фонды оценочных средств, позволяющие оценить уровень сформированности компетенций и результаты освоения дисциплины, представлены следующими компонентами:

Код оцениваемой компетенции (или) её части	Тип контроля	Вид контроля	Количество элементов, шт.
ПК-4	*текущий*	*устный опрос*	*1-15*
ПК-7			*1-15*
ПК-10			*1-16*
ПК-4	*промежуточный*	*компьютерный тест*	*33*
ПК-7			*33*
ПК-10			*34*

7.1. аттестации по итогам освоения дисциплины

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
Знает: Структура и содержание политики информационной безопасности; Основные направления реализации политики информационной безопасности (ПК-4);	1. При предпроектном обследовании системы защиты информации необходимо рассмотреть: все ресурсы, на которых хранится ценная информация; все сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом); отделы, к которым относятся ресурсы; виды ценной информации; парольная защита задачи управления компонентами системы ИБ 2. При предпроектном обследовании системы защиты информации необходимо рассмотреть: ущерб для каждого вида ценной информации по трем видам угроз: внешние, внутренние, комбинированные; бизнес-процессы, в которых обрабатывается информация; группы пользователей, имеющих доступ к ценной информации; класс группы пользователей; исключение нецелевого использования канальных и вычислительных ресурсов ИС аутентификация и идентификация

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
	3. При предпроектном обследовании системы защиты информации необходимо рассмотреть: доступ группы пользователей к информации; характеристики этого доступа (вид и права); средства защиты информации; средства защиты рабочего места группы пользователей. доступ из информационной системы компании к внешним Web-ресурсам обеспечение конфиденциальности информации при массовом использовании электронной почты, систем обмена мгновенными сообщениями 4. При определении уровня наносимого ущерба необходимо учитывать: стоимость возможных потерь при получении информации конкурентом; стоимость восстановления информации при ее утрате; затраты на восстановление нормального процесса функционирования АС и т.д. классификацию информационных ресурсов по степени важности/критичности лица; выявление должностных лиц, ответственных за целостность этих ресурсов; 5. При разработке модели угроз учитываются: внешние источники угроз внутренние источники угроз комбинированные источники угроз: внешние и внутренние, действующие совместно и/или согласованно. актуальные источники угроз на уровне бизнес-процессов: 6. При проведении диагностического обследования/аудита системы ИБ необходимо выполнить: классификацию информационных ресурсов по степени важности/критичности лица; выявление должностных лиц, ответственных за целостность этих ресурсов; доступ из информационной системы компании к внешним Web-ресурсам обеспечение конфиденциальности информации при массовом использовании электронной почты, систем обмена мгновенными сообщениями 7. При анализе СИБ на первых этапах построения СИБ необходимо: выявить организацию системы резервного копирования; определить требования к системе разделения прав доступа (пароли, разрешения), включая все правила доступа к информационной системе компании; провести предварительный анализ уязвимостей активного сетевого оборудования, серверов, рабочих станций, межсетевых экранов; выполнить оценку информационных рисков; обеспечение конфиденциальности информации при массовом использовании электронной почты, систем обмена мгновенными сообщениями 8. Анализ информационных рисков — это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков вероятный ущерб, который зависит от защищенности системы. построения модели информационной системы организации с точки зрения ИБ 9. Процесс анализа рисков включает в себя выполнение следующих групп задач:

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
	анализ ресурсов ИТ-инфраструктуры, включая информационные ресурсы, программные и технические средства, людские ресурсы, и построение модели ресурсов, учитывающей их взаимозависимости; анализ бизнес-процессов и групп задач, решаемых информационной системой, позволяющий оценить критичность ИТ-ресурсов, с учетом их взаимозависимостей; идентификация угроз безопасности в отношении ресурсов информационной системы и уязвимостей защиты, делающих возможным осуществление этих угроз; оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации; провести предварительный анализ уязвимостей активного сетевого оборудования, серверов, рабочих станций, межсетевых экранов; построения модели информационной системы организации с точки зрения ИБ 10. Процесс анализа рисков включает в себя выполнение следующих групп задач: определение величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость; ранжирование существующих рисков; разработка системы первоочередных мероприятий по уменьшению величины рисков до приемлемого уровня на основе проводимого анализа рисков. выявить организацию системы резервного копирования; определить требования к системе разделения прав доступа (пароли, разрешения), включая все правила доступа к информационной системе компании;
Умеет: Разрабатывать политики безопасности информации автоматизированных систем (ПК-4); Планировать политику безопасности программных компонентов автоматизированных систем (ПК-4);	14. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: подсистему защиты периметра сети и межсетевых взаимодействий (межсетевые экраны и т.п.); подсистему защиты серверов сети; средства защиты рабочих станций; подсистему мониторинга и аудита безопасности; подсистему контроля персонала. 15. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: средства обнаружения атак и автоматического реагирования; подсистему комплексной антивирусной защиты; средства анализа защищенности и управления политикой безопасности; средства контроля целостности данных; подсистему контроля инфраструктуры. 16. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: средства криптографической защиты информации; инфраструктуру открытых ключей; подсистему резервного копирования и восстановления данных; подсистему контроля инфраструктуры. подсистему контроля помещений. автоматизированную систему установки обновлений ПО; 17. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: подсистему управления ИБ; подсистему аутентификации и идентификации; подсистему контроля инфраструктуры. подсистему контроля телефонной сети. подсистему защиты внутренних сетевых ресурсов; 18. Интегрированная архитектура систем ИБ может включать в себя

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
	набор следующих подсистем: подсистему защиты Web-ресурсов; подсистему контроля содержимого Интернет-трафика; подсистему физической защиты. подсистему контроля персонала. подсистему контроля инфраструктуры. 19. Что такое политика информационной безопасности организации Набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию Уничтожение, модификация, копирование информации в организации Набор административных документов, утвержденных в организации Совокупность механизмов компьютерных систем Инструкции администраторам по настройке информационных систем 20. Типовые разделы Политики ИБ: «Цель политики». «Область применения». «Политика». Описывает сами требования ; идентификация угроз безопасности в отношении ресурсов информационной системы и уязвимостей защиты, делающих возможным осуществление этих угроз; оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации; 21. Типовые разделы Политики ИБ: «Ответственность». Описывает наказание за нарушение указанных в предыдущем разделе требований; «Термины и определения»; «История изменений данной политики». Дает возможность отследить все вносимые в документ изменения (дата, автор, краткая суть изменения). организация системы резервного копирования; требования к системе разделения прав доступа (пароли, разрешения), включая все правила доступа к информационной системе компании; 22. Согласно Оранжевой книге, политика безопасности должна включать в себя по крайней мере следующие элементы: произвольное управление доступом; безопасность повторного использования объектов; метки безопасности; принудительное управление доступом. соответствие политики безопасности действующему законодательству порядок разработки и сопровождения систем безопасность повторного использования объектов; метки безопасности; 23. С практической точки зрения политику безопасности целесообразно рассматривать на двух уровнях детализации. на трех уровнях детализации. на четырех уровнях детализации.
Имеет практический опыт: Формирования политики информационной безопасности в автоматизированных системах (ПК-4);	11. Назовите основные направления сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности. 12. Нарисуйте IDEF0 диаграмму взаимодействия подсистем обеспечения информационной безопасности.

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
Знает: Структуру и состав исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-7); Принципы построения систем защиты информации (ПК-7)	1. При предпроектном обследовании системы защиты информации необходимо рассмотреть: все ресурсы, на которых хранится ценная информация; все сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом); отделы, к которым относятся ресурсы; виды ценной информации; парольная защита задачи управления компонентами системы ИБ 2. При предпроектном обследовании системы защиты информации необходимо рассмотреть: ущерб для каждого вида ценной информации по трем видам угроз: внешние, внутренние, комбинированные; бизнес-процессы, в которых обрабатывается информация; группы пользователей, имеющих доступ к ценной информации; класс группы пользователей; исключение нецелевого использования канальных и вычислительных ресурсов ИС аутентификация и идентификация 3. При предпроектном обследовании системы защиты информации необходимо рассмотреть: доступ группы пользователей к информации; характеристики этого доступа (вид и права); средства защиты информации; средства защиты рабочего места группы пользователей. доступ из информационной системы компании к внешним Web-ресурсам обеспечение конфиденциальности информации при массовом использовании электронной почты, систем обмена мгновенными сообщениями 4. При определении уровня наносимого ущерба необходимо учитывать: стоимость возможных потерь при получении информации конкурентом; стоимость восстановления информации при ее утрате; затраты на восстановление нормального процесса функционирования АС и т.д. классификацию информационных ресурсов по степени важности/критичности лица; выявление должностных лиц, ответственных за целостность этих ресурсов; 5. При разработке модели угроз учитываются: внешние источники угроз внутренние источники угроз комбинированные источники угроз: внешние и внутренние, действующие совместно и/или согласованно. актуальные источники угроз на уровне бизнес-процессов: 6. При проведении диагностического обследования/аудита системы ИБ необходимо выполнить: классификацию информационных ресурсов по степени важности/критичности лица; выявление должностных лиц, ответственных за целостность этих ресурсов; доступ из информационной системы компании к внешним Web-ресурсам обеспечение конфиденциальности информации при массовом использовании электронной почты, систем обмена мгновенными сообщениями

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
	7. При анализе СИБ на первых этапах построения СИБ необходимо: выявить организацию системы резервного копирования; определить требования к системе разделения прав доступа (пароли, разрешения), включая все правила доступа к информационной системе компании; провести предварительный анализ уязвимостей активного сетевого оборудования, серверов, рабочих станций, межсетевых экранов; выполнить оценку информационных рисков; обеспечение конфиденциальности информации при массовом использовании электронной почты, систем обмена мгновенными сообщениями 8. Анализ информационных рисков — это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков вероятный ущерб, который зависит от защищенности системы. построения модели информационной системы организации с точки зрения ИБ 9. Процесс анализа рисков включает в себя выполнение следующих групп задач: анализ ресурсов ИТ-инфраструктуры, включая информационные ресурсы, программные и технические средства, людские ресурсы, и построение модели ресурсов, учитывающей их взаимозависимости; анализ бизнес-процессов и групп задач, решаемых информационной системой, позволяющий оценить критичность ИТ-ресурсов, с учетом их взаимозависимостей; идентификация угроз безопасности в отношении ресурсов информационной системы и уязвимостей защиты, делающих возможным осуществление этих угроз; оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации; провести предварительный анализ уязвимостей активного сетевого оборудования, серверов, рабочих станций, межсетевых экранов; построения модели информационной системы организации с точки зрения ИБ 10. Процесс анализа рисков включает в себя выполнение следующих групп задач: определение величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость; ранжирование существующих рисков; разработка системы первоочередных мероприятий по уменьшению величины рисков до приемлемого уровня на основе проводимого анализа рисков. выявить организацию системы резервного копирования; определить требования к системе разделения прав доступа (пароли, разрешения), включая все правила доступа к информационной системе компании;
Умеет: Собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-7); Проводить анализ структурных и функциональных схем защищенной автоматизированной системы (ПК-7);	14. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: подсистему защиты периметра сети и межсетевых взаимодействий (межсетевые экраны и т.п.); подсистему защиты серверов сети; средства защиты рабочих станций; подсистему мониторинга и аудита безопасности; подсистему контроля персонала. 15. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: средства обнаружения атак и автоматического реагирования; подсистему комплексной антивирусной защиты;

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
	средства анализа защищенности и управления политикой безопасности; средства контроля целостности данных; подсистему контроля инфраструктуры. 16. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: средства криптографической защиты информации; инфраструктуру открытых ключей; подсистему резервного копирования и восстановления данных; подсистему контроля инфраструктуры. подсистему контроля помещений. автоматизированную систему установки обновлений ПО; 17. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: подсистему управления ИБ; подсистему аутентификации и идентификации; подсистему контроля инфраструктуры. подсистему контроля телефонной сети. подсистему защиты внутренних сетевых ресурсов; 18. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: подсистему защиты Web-ресурсов; подсистему контроля содержимого Интернет-трафика; подсистему физической защиты. подсистему контроля персонала. подсистему контроля инфраструктуры. 19. Что такое политика информационной безопасности организации Набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию Уничтожение, модификация, копирование информации в организации Набор административных документов, утвержденных в организации Совокупность механизмов компьютерных систем Инструкции администраторам по настройке информационных систем 20. Типовые разделы Политики ИБ: «Цель политики». «Область применения». «Политика». Описывает сами требования ; идентификация угроз безопасности в отношении ресурсов информационной системы и уязвимостей защиты, делающих возможным осуществление этих угроз; оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации; 21. Типовые разделы Политики ИБ: «Ответственность». Описывает наказание за нарушение указанных в предыдущем разделе требований; «Термины и определения»; «История изменений данной политики». Дает возможность отследить все вносимые в документ изменения (дата, автор, краткая суть изменения). организация системы резервного копирования; требования к системе разделения прав доступа (пароли, разрешения), включая все правила доступа к информационной системе компании; 22. Согласно Оранжевой книге, политика безопасности должна включать в себя по крайней мере следующие элементы:

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
	произвольное управление доступом; безопасность повторного использования объектов; метки безопасности; принудительное управление доступом. соответствие политики безопасности действующему законодательству порядок разработки и сопровождения систем безопасность повторного использования объектов; метки безопасности; 23. С практической точки зрения политику безопасности целесообразно рассматривать на двух уровнях детализации. на трех уровнях детализации. на четырех уровнях детализации.
Имеет практический опыт: Сбора и и анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-7).	13. Назовите показатели анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности. 24. Назовите основные принципы формирования политики информационной безопасности в автоматизированных системах.

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
Знает: Методы анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)	1. При предпроектном обследовании системы защиты информации необходимо рассмотреть: все ресурсы, на которых хранится ценная информация; все сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом); отделы, к которым относятся ресурсы; виды ценной информации; парольная защита задачи управления компонентами системы ИБ 2. При предпроектном обследовании системы защиты информации необходимо рассмотреть: ущерб для каждого вида ценной информации по трем видам угроз: внешние, внутренние, комбинированные; бизнес-процессы, в которых обрабатывается информация; группы пользователей, имеющих доступ к ценной информации; класс группы пользователей; исключение нецелевого использования канальных и вычислительных ресурсов ИС аутентификация и идентификация 3. При предпроектном обследовании системы защиты информации необходимо рассмотреть: доступ группы пользователей к информации; характеристики этого доступа (вид и права); средства защиты информации; средства защиты рабочего места группы пользователей. доступ из информационной системы компании к внешним Web-ресурсам обеспечение конфиденциальности информации при массовом использовании электронной почты, систем обмена мгновенными сообщениями 4. При определении уровня наносимого ущерба необходимо учитывать: стоимость возможных потерь при получении информации конкурентом; стоимость восстановления информации при ее утрате; затраты на восстановление нормального процесса

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
	функционирования АС и т.д. классификацию информационных ресурсов по степени важности/критичности лица; выявление должностных лиц, ответственных за целостность этих ресурсов; 5. При разработке модели угроз учитываются: внешние источники угроз внутренние источники угроз комбинированные источники угроз: внешние и внутренние, действующие совместно и/или согласованно. актуальные источники угроз на уровне бизнес-процессов: 6. При проведении диагностического обследования/аудита системы ИБ необходимо выполнить: классификацию информационных ресурсов по степени важности/критичности лица; выявление должностных лиц, ответственных за целостность этих ресурсов; доступ из информационной системы компании к внешним Web-ресурсам обеспечение конфиденциальности информации при массовом использовании электронной почты, систем обмена мгновенными сообщениями 7. При анализе СИБ на первых этапах построения СИБ необходимо: выявить организацию системы резервного копирования; определить требования к системе разделения прав доступа (пароли, разрешения), включая все правила доступа к информационной системе компании; провести предварительный анализ уязвимостей активного сетевого оборудования, серверов, рабочих станций, межсетевых экранов; выполнить оценку информационных рисков; обеспечение конфиденциальности информации при массовом использовании электронной почты, систем обмена мгновенными сообщениями 8. Анализ информационных рисков — это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков вероятный ущерб, который зависит от защищенности системы. построения модели информационной системы организации с точки зрения ИБ 9. Процесс анализа рисков включает в себя выполнение следующих групп задач: анализ ресурсов ИТ-инфраструктуры, включая информационные ресурсы, программные и технические средства, людские ресурсы, и построение модели ресурсов, учитывающей их взаимозависимости; анализ бизнес-процессов и групп задач, решаемых информационной системой, позволяющий оценить критичность ИТ-ресурсов, с учетом их взаимозависимостей; идентификация угроз безопасности в отношении ресурсов информационной системы и уязвимостей защиты, делающих возможным осуществление этих угроз; оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации; провести предварительный анализ уязвимостей активного сетевого оборудования, серверов, рабочих станций, межсетевых экранов; построения модели информационной системы организации с точки зрения ИБ 10. Процесс анализа рисков включает в себя выполнение следующих групп задач:

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
	определение величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость; ранжирование существующих рисков; разработка системы первоочередных мероприятий по уменьшению величины рисков до приемлемого уровня на основе проводимого анализа рисков. выявить организацию системы резервного копирования; определить требования к системе разделения прав доступа (пароли, разрешения), включая все правила доступа к информационной системе компании;
Умеет: Проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)	14. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: подсистему защиты периметра сети и межсетевых взаимодействий (межсетевые экраны и т.п.); подсистему защиты серверов сети; средства защиты рабочих станций; подсистему мониторинга и аудита безопасности; подсистему контроля персонала. 15. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: средства обнаружения атак и автоматического реагирования; подсистему комплексной антивирусной защиты; средства анализа защищенности и управления политикой безопасности; средства контроля целостности данных; подсистему контроля инфраструктуры. 16. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: средства криптографической защиты информации; инфраструктуру открытых ключей; подсистему резервного копирования и восстановления данных; подсистему контроля инфраструктуры. подсистему контроля помещений. автоматизированную систему установки обновлений ПО; 17. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: подсистему управления ИБ; подсистему аутентификации и идентификации; подсистему контроля инфраструктуры. подсистему контроля телефонной сети. подсистему защиты внутренних сетевых ресурсов; 18. Интегрированная архитектура систем ИБ может включать в себя набор следующих подсистем: подсистему защиты Web-ресурсов; подсистему контроля содержимого Интернет-трафика; подсистему физической защиты. подсистему контроля персонала. подсистему контроля инфраструктуры. 19. Что такое политика информационной безопасности организации Набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию Уничтожение, модификация, копирование информации в организации Набор административных документов, утвержденных в организации Совокупность механизмов компьютерных систем Инструкции администраторам по настройке информационных систем

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
	20. Типовые разделы Политики ИБ: «Цель политики». «Область применения». «Политика». Описывает сами требования ; идентификация угроз безопасности в отношении ресурсов информационной системы и уязвимостей защиты, делающих возможным осуществление этих угроз; оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации; 21. Типовые разделы Политики ИБ: «Ответственность». Описывает наказание за нарушение указанных в предыдущем разделе требований; «Термины и определения»; «История изменений данной политики». Дает возможность отследить все вносимые в документ изменения (дата, автор, краткая суть изменения). организация системы резервного копирования; требования к системе разделения прав доступа (пароли, разрешения), включая все правила доступа к информационной системе компании; 22. Согласно Оранжевой книге, политика безопасности должна включать в себя по крайней мере следующие элементы: произвольное управление доступом; безопасность повторного использования объектов; метки безопасности; принудительное управление доступом. соответствие политики безопасности действующему законодательству порядок разработки и сопровождения систем безопасность повторного использования объектов; метки безопасности; 23. С практической точки зрения политику безопасности целесообразно рассматривать на двух уровнях детализации. на трех уровнях детализации. на четырех уровнях детализации.
Имеет практический опыт: анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10).	25. Приведите структуру основных политик информационной безопасности. 26. Приведите состав политики информационной безопасности организации.

7.2. Методические рекомендации к определению процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Рабочая учебная программа дисциплины содержит следующие структурные элементы:

- перечень компетенций, формируемых в результате изучения дисциплины в процессе освоения образовательной программы;

- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности в процессе освоения образовательной программы (далее–задания). Задания по каждой компетенции, как правило, не должны повторяться.

Требования по формированию задания на оценку ЗНАНИЙ:

- обучающийся должен воспроизводить и объяснять учебный материал с требуемой степенью научной точности и полноты;

- применяются средства оценивания компетенций: тестирование, вопросы по основным понятиям дисциплины и т.п.

Требования по формированию задания на оценку УМЕНИЙ:

- обучающийся должен решать типовые задачи (выполнять задания) на основе воспроизведения стандартных алгоритмов решения;

- применяются следующие средства оценивания компетенций: простые ситуационные задачи (задания) с коротким ответом или простым действием, упражнения, задания на соответствие или на установление правильной последовательности, эссе и другое.

Требования по формированию задания на оценку навыков и (или) ОПЫТА ДЕЯТЕЛЬНОСТИ:

- обучающийся должен решать усложненные задачи (выполнять задания) на основе приобретенных знаний, умений и навыков, с их применением в определенных ситуациях;

- применяются средства оценивания компетенций: задания требующие многошаговых решений как в известной, так и в нестандартной ситуациях, задания, требующие поэтапного решения и развернутого ответа, ситуационные задачи, проектная деятельность, задания расчетно-графического типа. Средства оценивания компетенций выбираются в соответствии с заявленными результатами обучения по дисциплине.

Процедура выставления оценки доводится до сведения обучающихся в течение месяца с начала изучения дисциплины путем ознакомления их с технологической картой дисциплины, которая является неотъемлемой частью рабочей учебной программы по дисциплине.

В результате оценивания компетенций по дисциплине студенту начисляются баллы по шкале, указанной в рабочей учебной программе по дисциплине.

7.3. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Успешность усвоения дисциплины характеризуется качественной оценкой на основе листа оценки сформированности компетенций, который является приложением к зачетно-экзаменационной ведомости при проведении промежуточной аттестации по дисциплине.

Критерии оценивания компетенций

Компетенция считается сформированной, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует *повышенному уровню* сформированности компетенции.

Компетенция считается сформированной, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует *пороговому уровню* сформированности компетенции.

Компетенция считается несформированной, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет практические работы, не демонстрирует необходимых умений, доля невыполненных заданий, предусмотренных рабочей учебной программой составляет 55 %, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует *допороговому уровню*.

Шкала оценки уровня освоения дисциплины

Качественная оценка может быть выражена: в процентном отношении качества усвоения дисциплины, которая соответствует баллам, и переводится в уровневую шкалу и оценки «отлично» / 5, «хорошо» / 4, «удовлетворительно» / 3, «неудовлетворительно» / 2, «зачтено», «не

зачтено». Преподаватель ведет письменный учет текущей успеваемости студента в соответствии с технологической картой по дисциплине.

Шкала оценки результатов освоения дисциплины, сформированности компетенций

Шкалы оценки уровня сформированности компетенции (й)		Шкала оценки уровня освоения дисциплины		
Уровневая шкала оценки компетенций	*100 балльная шкала, %*	*100 балльная шкала, %*	*5-балльная шкала, дифференцированная оценка/балл*	*Недифференцированная оценка*
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
пороговый	61-85,9	70-85,9	«хорошо» / 4	зачтено
		61-69,9	«удовлетворительно» / 3	зачтено
повышенный	86-100	86-100	«отлично» / 5	зачтено

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Списки основной литературы

1. Баранова, Е. К. Моделирование системы защиты информации. Практикум [Электронный ресурс] : учеб. пособие для вузов по направлению "Приклад. информатика" / Е. К. Баранова, А. В. Бабаш. - Изд. 2-е, перераб. и доп. - Документ Bookread2. - М. : РИОР [и др.], 2018. - 223 с. - Режим доступа: http://znanium.com/bookread2.php?book=916068

2. Варфоломеева, А. О. Информационные системы предприятия [Электронный ресурс] : учеб. пособие для вузов по направлению 09.03.03. "Приклад. информатика" и др. экон. специальностям / А. О. Варфоломеева, А. В. Коряковский, В. П. Романов. - 2-е изд., перераб. и доп. - Документ Bookread2. - М. : ИНФРА-М, 2019. - 330 с. - Режим доступа: http://znanium.com/bookread2.php?book=1002067

3. Заботина, Н. Н. Проектирование информационных систем [Электронный ресурс] : учеб. пособие для вузов по специальности 09.03.03 "Приклад. информатика (по обл.)" и др. экон. специальностям / Н. Н. Заботина. - Документ Bookread2. - М. : ИНФРА-М, 2016. - 331 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=542810

4. Коваленко, В. В. Проектирование информационных систем [Электронный ресурс] : учеб. пособие для студентов (бакалавров и специалистов) вузов по направлению 09.03.03 "Приклад. информатика" / В. В. Коваленко. - Документ Bookread2. - М. : Форум, 2018. - 319 с. : ил., табл. - Режим доступа: http://znanium.com/bookread2.php?book=980117

5. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учеб. пособие для вузов по направлению 09.03.01 "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ Bookread2. - М. : ФОРУМ [и др.], 2018. - 592 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=937502

Списки дополнительной литературы

6. Башлы, П. Н. Информационная безопасность[Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Документ Bookread2. - М. : РИОР, 2013. - 222 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=405000#

7. Жукова, М. Н. Управление информационной безопасностью [Электронный ресурс] : учеб. пособие по направлениям "Информ. безопасность", "Информатика и вычисл. техника", "Информ. системы" : в 3 ч. Ч. 2 Управление инцидентами информационной безопасности / М. Н. Жукова, В. Г. Жуков, В. В. ЗолотаревСиб. гос. аэрокосм. ун-т им. акад. М. Ф. Решетнева. - Документ HTML. - Красноярск : Сиб. гос. аэрокосм. ун-т, 2012. - 100 с. - Режим доступа: http://znanium.com/bookread.php?book=463061

8. Корячко, В. П. Процессы и задачи управления проектами информационных систем [Текст] : учеб. пособие для студентов вузов по направлению подгот. 230100 "Информатика и вычисл. техника" / В. П. Корячко, А. И. Таганов. - М. : Горячая линия -Телеком, 2014. - 376 с. : табл.

9. Малюк, А. А. Теория защиты информации [Текст] / А. А. Малюк. - М. : Горячая линия - Телеком, 2013. - 184 с. : табл.

10. Мельников, Д. А. Информационная безопасность открытых систем [Текст] : учеб. для студентов по направлению "Приклад. информатика" / Д. А. Мельников. - М. : Флинта [и др.], 2013. - 442 с. : табл.

8.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее – сеть "Интернет"), необходимых для освоения дисциплины

1. ИНТУИТ. Национальный открытый университет [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/. – Загл. с экрана.
2. Российское образование [Электронный ресурс] : федер. портал. - Режим доступа: http://www.edu.ru. - Загл. с экрана.
3. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. - Режим доступа: http://elib.tolgas.ru/. - Загл. с экрана.
4. Электронно-библиотечная система Znanium.com [Электронный ресурс]. - Режим доступа: http://znanium.com/. - Загл. с экрана.
5. Защита информации. Инсайд [Электронный ресурс]. – Режим доступа: http://www.inside-zi.ru/. – Загл. с экрана.
6. Information Security/Информационная безопасность [Электронный ресурс]. – Режим доступа: http://www.itsec.ru/insec-about.php. - Загл. с экрана.
7. Информационная безопасность банков [Электронный ресурс]. – Режим доступа: http://www.ib-bank.ru/. – Загл. с экрана.
8. Лаборатория Сетевой Безопасности [Электронный ресурс]. – Режим доступа: http://ypn.ru/. – Загл. с экрана.
9. Information Security [Электронный ресурс]. – Режим доступа: http://www.net-security.org/insecuremag.php. - Загл. с экрана.
10. Бизнес без опасности [Электронный ресурс]. – Режим доступа: http://lukatsky.blogspot.ru/. – Загл. с экрана.
11. Проектирование системы обеспечения информационной безопасности [Электронный ресурс]. – Режим доступа: http://itzashita.ru/designing/proektirovanie-sistemy-obespecheniya-informacionnoj-bezopasnosti.html. - Загл. с экрана.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Краткая характеристика применяемого программного обеспечения

№ п/п	Программный продукт	Характеристика	Назначение при освоении дисциплины
1	MS Word	текстовый редактор	Выполнение практических работ, выполнение курсового проекта
2	Microsoft Excel	табличный процессор	Выполнение практических работ
3	Internet Explorer	обозреватель Интернет	Выполнение практических работ, выполнение курсового проекта

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа используются специальные помещения - учебные аудитории, укомплектованные специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации.

Для проведения практических занятий (занятий семинарского типа), групповых и индивидуальных консультаций используются специальные помещения - учебные аудитории, укомплектованные специализированной мебелью и техническими средствами обучения.

Для проведения лабораторных работ используются аудитория информационных технологий, информатики и методов программирования и лаборатория информационных технологий, информатики и методов программирования, оснащенные лабораторным оборудованием различной степени сложности

Для текущего контроля и промежуточной аттестации используются специальные помещения - учебные аудитории, укомплектованные специализированной мебелью, и (или) компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета.

Для самостоятельной работы обучающихся используются специальные помещения - учебные аудитории для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета.

11. Примерная технологическая карта дисциплины «Эксплуатация систем информационной безопасности»

Кафедра «Прикладная информатика в экономике», преподаватель _____

направление подготовки 10.03.01 «Информационная безопасность»

№	Виды контрольных точек	Кол-во контр. точек	Кол-во баллов за 1 контр. точку	График прохождения контрольных точек																**Зачетно - экзаменационная сессия**
				Сентябрь				Октябрь				Ноябрь				Декабрь				
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
1																				
1.1	Практическая работа № 1.	1	9			+														
1.2	Практическая работа № 2.	1	9					+												
1.3	Практическая работа № 3.	1	9							+										
1.4	Практическая работа № 4.	1	9									+								
1.5	Практическая работа № 5.	1	9											+						
1.6	Практическая работа № 6.	1	9													+				
1.8	Посещаемость лекций	16	1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
1.9	Курсовой проект	1	20																+	
	Итого:		90																	
2.	Творческий рейтинг																			
2.1	Участие в олимпиадах, конкурсах и т.д.	1	10																+	
	Итого:		100																	
	экзамен																			экзамен