МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)
Филиал РГГУ в г. Домодедово

Кафедра математических и естественнонаучных дисциплин

Б1.В.04 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 38.03.02 «Менеджмент»
Направленность (профиль) «Менеджмент организации»
Уровень высшего образования «бакалавриат»

Форма обучения очная, очно-заочная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Домодедово 2023

Информационная безопасность

Рабочая программа дисциплины

Составитель:
к.п.н. Козлов В.Г.

УТВЕРЖДЕНО
Протокол заседания кафедры
Математических и естественнонаучных дисциплин
филиала РГГУ в г. Домодедово
№ 5 от 29.03.2023г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Рабочая программа учебной дисциплины является частью образовательной программы бакалавриата по направлению подготовки 38.03.02 «Менеджмент», направление – «Менеджмент организации».

Цель освоения учебной дисциплины:

ознакомление обучающихся с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей, и, конечно, методов их применения.

Задачи изучения дисциплины «Информационная безопасность»:

- сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;
- передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;
- сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

Содержание дисциплины охватывает круг вопросов, связанных с политикой безопасности организации и правовых и организационных методах защиты компьютерной информации; основные понятия и определения защиты информации; методах и средствах защиты компьютерной информации.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4.3 Использует информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач для достижения профессиональных целей на государственном и иностранном (-ых) языках	*Знать:* стандартные коммуникативные задачи для достижения профессиональных целей на государственном и иностранном (-ых) языках *Уметь:* использовать коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач *Владеть:* навыками использования информационно-коммуникационных технологий при поиске необходимой информации в процессе решения стандартных коммуникативных

		задач для достижения профессиональных целей на государственном и иностранном (-ых) языках
ПК-2 Способен регламентировать процессы подразделений организации	ПК-2.3 Вводит в действие регламент процесса подразделения организации	*Знать:* механизм ввода в действие регламента процесса подразделения организации *Уметь:* вводить в действие регламент процесса подразделения организации *Владеть:* навыками ввода в действие регламента процесса подразделения организации
	ПК-2.4 Осуществляет контроль выполнения регламента процесса подразделения организации	*Знать:* механизм контроля выполнения регламента процесса подразделения организации *Уметь:* контролировать выполнение регламента процесса подразделения организации *Владеть:* навыками осуществления контроля выполнения регламента процесса подразделения организации

1.3. Место учебной дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» входит в вариативную часть Блока 1. Дисциплины (модули) программы подготовки студентов по направлению подготовки 38.03.02 «Менеджмент» направленность «Менеджмент организации».

Изучению дисциплины «Информационная безопасность» предшествует изучение дисциплины: «Информатика».

2. Структура дисциплины

Для очной формы обучения набор 2023

Общая трудоёмкость дисциплины составляет 3 зачетных единицы, 108 ч., в том числе контактная работа обучающихся с преподавателем 42 ч., самостоятельная работа обучающихся 66 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)				Формы текущего контроля успеваемости, форма промежуточной аттестации
			Контактная		Промежуточная аттестация	Самостоятельная работа	
			Лекции	Практические занятия			
Раздел I. Основы информационной безопасности							
1	Понятие информационной безопасности. Основные составляющие	7	2	3		6	Проверочная работа Вопросы к зачету с оценкой
2	Наиболее распространенные угрозы информационной безопасности и её составляющие	7	1	3		7	Тестирование Вопросы к зачету с оценкой
Раздел II. Уровни информационной безопасности							
3	Законодательный уровень информационной безопасности	7	1	2		7	Тестирование Вопросы к зачету с оценкой
4	Административный уровень информационной безопасности	7	2	3		6	Тестирование Вопросы к зачету с оценкой
5	Процедурный уровень информационной безопасности	7	1	3		7	Тестирование Вопросы к зачету с оценкой
Раздел III. Программно-технические меры по обеспечению информационной безопасности							
6	Основные характеристики программно-технических мер	7	1	3		7	Тестирование Вопросы к зачету с оценкой
7	Идентификация и аутентификация	7	1	3		7	Проверочная работа Вопросы к зачету с оценкой
8	Протоколирование и аудит, шифрование,	7	2	3		7	Проверочная работа

	контроль целостности						Вопросы к зачету с оценкой
9	Экранирование, анализ защищенности	7	2	3		6	Тестирование Вопросы к зачету с оценкой
10	Обеспечение высокой доступности	7	1	2		6	Проверочная работа Вопросы к зачету с оценкой
	Зачет с оценкой	7					
	Итого:		14	28		66	

Для очно-заочной формы обучения набор 2023

Общая трудоёмкость дисциплины составляет 3 зачетных единицы, 108 ч., в том числе контактная работа обучающихся с преподавателем 24 ч, самостоятельная работа обучающихся 84 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)				Формы текущего контроля успеваемости, форма промежуточной аттестации
			Контактная		Промежуточная аттестация	Самостоятельная работа	
			Лекции	Практические занятия			
Раздел I. Основы информационной безопасности							
1	Понятие информационной безопасности. Основные составляющие	7	1	2		8	Проверочная работа Вопросы к зачету с оценкой
2	Наиболее распространенные угрозы информационной безопасности и её составляющие	7	1	1		9	Тестирование Вопросы к зачету с оценкой
Раздел II. Уровни информационной безопасности							
3	Законодательный уровень информационной безопасности	7	1	1		8	Тестирование Вопросы к зачету с оценкой
4	Административный уровень информационной безопасности	7	1	2		9	Тестирование Вопросы к зачету с оценкой
5	Процедурный уровень информационной безопасности	7	1	1		8	Тестирование Вопросы к зачету с оценкой
Раздел III. Программно-технические меры по обеспечению информационной безопасности							
6	Основные характеристики программно-технических мер	7	1	1		9	Тестирование Вопросы к зачету с оценкой
7	Идентификация и аутентификация	7	1	1		8	Проверочная работа Вопросы к зачету с оценкой
8	Протоколирование и аудит, шифрование,	7	1	2		8	Проверочная работа

	контроль целостности						Вопросы к зачету с оценкой
9	Экранирование, анализ защищенности	7	1	2		8	Тестирование Вопросы к зачету с оценкой
10	Обеспечение высокой доступности	7	1	1		9	Проверочная работа Вопросы к зачету с оценкой
	Зачет с оценкой	7					
	Итого:		10	14		84	

3. Содержание дисциплины

РАЗДЕЛ I. Основы информационной безопасности

Тема 1. Понятие информационной безопасности. Основные составляющие

Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.

Тема 2. Наиболее распространенные угрозы информационной безопасности и её составляющие

Основные определения и критерии классификации угроз. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности*.

РАЗДЕЛ II. Уровни информационной безопасности

Тема 3. Законодательный уровень информационной безопасности

Российское законодательство в области информационной безопасности. Стандарты и спецификации в области информационной безопасности.

Тема 4. Административный уровень информационной безопасности

Основные понятия, политика безопасности. Жизненный цикл информационной системы. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.

Тема 5. Процедурный уровень информационной безопасности

Основные классы мер процедурного уровня. Управление персоналом. Физическая защита*. Поддержание работоспособности. Реагирование на нарушения режима безопасности*. Планирование восстановительных работ.

РАЗДЕЛ III. Программно-технические меры по обеспечению информационной безопасности

Тема 6. Основные характеристики программно-технических мер

Основные понятия программно-технического уровня. Архитектурная безопасность. Экранирование. Анализ защищённости. Отказоустойчивость*. Безопасное восстановление.

Тема 7. Идентификация и аутентификация

Основные понятия. Парольная аутентификация. Одноразовые пароли. Идентификация/аутентификация с помощью биометрических данных*. Управление доступом. Ролевое управление доступом.

Тема 8. Протоколирование и аудит, шифрование, контроль целостности

Основные понятия. Активный аудит. Шифрование*. Симметричный метод шифрования. Асимметричный метод шифрования. Секретный и открытый ключ.

Криптография. Контроль целостности*. Цифровые сертификаты. Электронная цифровая подпись.

Тема 9. Экранирование, анализ защищенности

Основные понятия. Экранирование. Фильтрация. Межсетевые экраны. Классификация межсетевых экранов. Архитектурная безопасность*. Транспортное экранирование. Анализ защищенности. База данных уязвимостей. Сетевой сканер*. Антивирусная защита.

Тема 10. Обеспечение высокой доступности

Эффективность услуг. Время недоступности. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Обеспечение обслуживаемости. Туннелирование.

4. Образовательные технологии

При реализации программы дисциплины «Информационная безопасность» используются различные образовательные технологии: аудиторные занятия проводятся в виде лекций и практических занятий. Лекции проводятся по типу проблемных лекций, лекций-визуализаций, лекций-дискуссий, лекций с применением техники обратной связи, лекций с разбором конкретных ситуаций.

Практических занятиях, проводимых по типу занятие-дискуссия, занятие – круглый стол, занятие - развернутая беседа с обсуждением докладов, предусмотрено обсуждение основополагающих и наиболее сложных вопросов курса, заслушивание докладов. Темы практических занятий отражают последовательность изучения курса в соответствии с программой.

Самостоятельная работа студентов подразумевает подготовку докладов, самоконтроль, подготовку к тестированию, работу с нормативно-правовыми актами и информационными ресурсами. Для самостоятельной работы студентов подготовлены задания для самостоятельной работы, список источников и литературы.

№ п/п	Наименование темы	Виды учебной работы	Образовательные технологии
1	2	3	5
1.	Понятие информационной безопасности. Основные составляющие	Лекция 1.	Вводная лекция
		Практическое занятие 1.	Обсуждение выступлений на практическом занятии
2.	Наиболее распространенные угрозы информационной безопасности и её составляющие	Лекция 1.	Проблемная лекция
		Практическое занятие 1.	Тестирование
3.	Законодательный уровень информационной безопасности	Лекция 2.	Лекция-дискуссия
		Практическое занятие 2.	Обсуждение выступлений на практическом занятии
4.	Административный уровень информационной безопасности	Лекция 2.	Лекция с разбором конкретной ситуации
		Практическое занятие 2.	Дискуссия на практическом занятии
5.	Процедурный уровень информационной безопасности	Лекция 2.	Лекция с применением техники обратной связи
		Практическое занятие 2.	Практическое занятие - развернутая беседа с обсуждением докладов
6.	Основные характеристики программно-технических мер	Лекция 3.	Лекция-дискуссия
		Практическое занятие 3.	Дискуссия на практическом занятии
7.	Идентификация и аутентификация	Лекция 3.	Проблемная лекция
		Практическое занятие 7.	Практическое занятие - развернутая беседа с обсуждением докладов
8.	Протоколирование и аудит, шифрование, контроль целостности	Лекция 5.	Лекция с применением техники обратной связи

		Практическое занятие 8.	Дискуссия на практическом занятии
9.	Экранирование, анализ защищенности	Лекция 6.	Проблемная лекция
		Практическое занятие 9.	Тестирование
10.	Обеспечение высокой доступности	Лекция 7.	Лекция - визуализация
		Практическое занятие 10.	Дискуссия на практическом занятии

Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Наименование темы	Наименование оценочного средства
1	УК-4.3	Тема 1. Понятие информационной безопасности. Основные составляющие Тема 2. Наиболее распространенные угрозы информационной безопасности и её составляющие	Выступление на круглом столе Доклады Тестирование Проверочная работа Зачет с оценкой
2	ПК-2.3	Тема 3. Законодательный уровень информационной безопасности Тема 4. Административный уровень информационной безопасности Тема 5. Процедурный уровень информационной безопасности Тема 6. Основные характеристики программно-технических мер	Выступление на круглом столе Доклады Тестирование Проверочная работа Зачет с оценкой
3	ПК-2.4	Тема 7. Идентификация и аутентификация Тема 8. Протоколирование и аудит, шифрование, контроль целостности Тема 9. Экранирование, анализ защищенности Тема 10. Обеспечение высокой доступности	Выступление на круглом столе Доклады Тестирование Проверочная работа Зачет с оценкой

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Максимальное количество баллов за одну работу**	**Максимальное количество баллов всего**
Посещение лекций	2	20
Участие в обсуждении теоретических вопросов на круглых столах	5	10
Тестирование	5	10
Проверочная работа	20	20
Всего за текущий контроль		60
Зачет с оценкой		40
Итого за семестр		100

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/A,B	«отлично»/» зачтено (отлично»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.

		Компетенции, закреплённые за дисциплиной ,сформированы на уровне - «высокий».
82-68/C	«хорошо»/» зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне - «хороший».
67-50/D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной ,сформированы на уровне - «достаточный».
49-0/F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Примерные темы проверочных работ

1. Информационные ресурсы, подлежащие защите в сфере финансовой деятельности.
2. Классификация угроз информационной безопасности и их сравнительный анализ.
3. Информационная безопасность в современных условиях хозяйствования. Общегосударственные цели, задачи и методы обеспечения информационной безопасности.
4. Понятия о видах вирусов. Классификация вирусов и угрозы для информационной инфраструктуры хозяйствующих субъектов.
5. Вида возможных нарушений информационной безопасности в сфере финансовой деятельности.
6. Отечественные и международные стандарты обеспечения информационной безопасности.
7. Особенности современной нормативно-правовой и методологической базы обеспечения информационной безопасности.
8. Основные нормативные руководящие документы, касающиеся конфиденциальной информации и государственной тайны, нормативно-справочные документы по обеспечению информационной безопасности применяемые в финансовой деятельности.
9. Общие критерии оценки безопасности информационных систем и технологий ГОСТ 15408, как основа определения требований к обеспечению информационной безопасности.
10. Место информационной безопасности экономических систем в национальной безопасности страны.
11. Цели и задачи обеспечения национальной безопасности. Система целеполагания в структуре государственного и муниципального управления при обеспечении информационной безопасности.
12. Основные положения концепции информационной безопасности. Сравнительная таблица.
13. Государственные информационные ресурсы, подлежащие защите в сфере финансовой деятельности.
14. Взаимосвязь государственных и коммерческих информационных ресурсов (конфиденциальной информации и государственной тайны).
15. Модели безопасности, и их применение.
16. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Оценка системы защиты информации.
17. Оценка эффективности средств и механизмов обеспечения информационной безопасности.
18. Методы анализа способов нарушений информационной безопасности.
19. Программно-аппаратные комплексы криптографической защиты, их характеристики и особенности применения. Сравнительная таблица.
20. Нормативно-правовая база криптографической защиты.
21. ЭЦП и особенности работы в системах государственного и муниципального управления.

Тестовые задания к разделу 1

1. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется

1. актуальностью информации
2. доступностью
3. качеством информации
4. целостностью

2. Согласно «Оранжевой книге» минимальную защиту имеет группа критериев

1. C
2. A
3. B
4. D

3. Организационные требования к системе защиты

1. управленческие и идентификационные
2. административные и аппаратурные
3. административные и процедурные
4. аппаратурные и физические

4. Основу политики безопасности составляет

1. программное обеспечение
2. управление риском
3. способ управления доступом
4. выбор каналов связи

5. **Соответствие средств безопасности решаемым задачам характеризует**

1. эффективность
2. корректность
3. адекватность
4. унификация

6. С точки зрения ФСТЭК основной задачей средств безопасности является обеспечение сохранности информации

1. защиты от НСД
2. простоты реализации
3. надежности функционирования

7. Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне

1. E5
2. E7
3. E4
4. E6

8. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это

1. аудит
2. аутентификация
3. авторизация
4. идентификация

9. Согласно «Оранжевой книге» уникальные идентификаторы должны иметь

1. наиболее важные субъекты

2. наиболее важные объекты
3. все субъекты
4. все объекты

10. Соответствие средств безопасности решаемым задачам характеризует
1. эффективность
2. корректность
3. адекватность
4. унификация

11. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется
1. системой защиты
2. стандартом безопасности
3. профилем безопасности
4. профилем защиты

12. Для решения проблемы правильности выбора и надежности функционирования средств защиты в «европейских критериях» вводится понятие
1. унификации средств защиты
2. надежности защиты информации
3. адекватности средств защиты
4. оптимизации средств защиты

Тестовые задания к разделу 2

1. Организационные требования к системе защиты
1. управленческие и идентификационные
2. административные и аппаратурные
3. административные и процедурные
4. аппаратурные и физические

2. Основу политики безопасности составляет
1. программное обеспечение
2. управление риском
3. способ управления доступом
4. выбор каналов связи

3. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности
1. Лендвера
2. С полным перекрытием
3. Белла-ЛаПадула
4. На основе анализа угроз

4. Из перечисленного услуга защиты целостности доступна на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

1. 1, 2, 5
2. 1, 3, 5
3. 1, 2, 3
4. 4, 5, 6

5. Присвоение субъектам и объектам доступа уникального номера, шифра, ключа и

т.п. с целью получения доступа к информации — это

1. идентификация
2. аудит
3. авторизация
4. аутентификация

6. Из перечисленного типами услуг аутентификации являются:
1) идентификация;
2) достоверность происхождения данных;
3) достоверность объектов коммуникации;
4) причастность;
1. 3, 4
2. 1, 4
3. 2, 3
4. 1, 2

7. Как предотвращением неавторизованного использования ресурсов определена услуга защиты
1. аутентификация
2. причастность
3. контроль доступа
4. целостность

8. Пользовательское управление данными реализуется на уровне модели взаимодействия открытых систем
представления данных
1. канальном
2. сеансовом
3. прикладном

Тестовые задания к разделу 3

1. Наукой, изучающей математические методы защиты информации путем ее преобразования, является
1. криптоанализ
2. криптология
3. стеганография
4. криптография

2. Конечное множество используемых для кодирования информации знаков называется
1. шифром
2. кодом
3. алфавитом
4. ключом

3. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет
1. криптология
2. стеганография
3. криптоанализ
4. криптография

4. Обеспечением скрытности информации в информационных массивах занимается

1. криптография
2. криптоанализ
3. криптология
4. стеганография

5. Два ключа используются в криптосистемах

1. с открытым ключом
2. с закрытым ключом
3. двойного шифрования
4. симметричных

6. Главным параметром криптосистемы является показатель

1. безошибочности шифрования
2. скорости шифрования
3. криптостойкости
4. надежности функционирования

7. Длина исходного ключа в ГОСТ 28147-89 (бит)

1. 128
2. 256
3. 64

8. Основной целью системы брандмауэра является управление доступом

1. к архивам
2. внутри защищаемой сети
3. к секретной информации
4. к защищаемой сети

9. Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки
адресов отправителя и получателя

1. содержания сообщений
2. электронной подписи
3. структуры данных

10. Из перечисленного система брандмауэра может быть: 1) репитором; 2) маршрутизатором; 3) ПК; 4) хостом; 5) ресивером

1. 3, 4, 5
2. 2, 3, 4
3. 1, 4, 5
4. 1, 2, 3

Примерный перечень вопросов для подготовки к зачету с оценкой

1. Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб.
2. Доступность, целостность, конфиденциальность.
3. Компьютерное преступление, жизненный цикл информационных систем.
4. Сложные системы. Структурный подход.

5. Основные определения и критерии классификации угроз.
6. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.
7. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
8. Российское законодательство в области информационной безопасности.
9. Зарубежное законодательство в области информационной безопасности.
10. Стандарты и спецификации в области информационной безопасности.
11. Основные понятия, политика безопасности.
12. Жизненный цикл информационной системы.
13. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.
14. Основные классы мер процедурного уровня.
15. Управление персоналом. Физическая защита.
16. Поддержание работоспособности.
17. Реагирование на нарушения режима безопасности.
18. Планирование восстановительных работ.
19. Основные понятия программно-технического уровня. Архитектурная безопасность.
20. Экранирование. Анализ защищённости.
21. Отказоустойчивость. Безопасное восстановление.
22. Основные понятия криптографии.
24. Парольная аутентификация. Одноразовые пароли.
25. Идентификация/аутентификация с помощью биометрических данных.
26. Управление доступом. Ролевое управление доступом.
27. Активный аудит. Шифрование.
28. Симметричный метод шифрования.
29. Асимметричный метод шифрования.
30. Секретный и открытый ключ.
31. Криптография. Контроль целостности
32. Цифровые сертификаты.
33. Электронная цифровая подпись.
34. Экранирование. Фильтрация. Межсетевые экраны.
35. Классификация межсетевых экранов.
36. Архитектурная безопасность.
37. Транспортное экранирование. Анализ защищенности.
38. Сетевой сканер. Антивирусная защита.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями от 25 ноября, 27 декабря 2009 г.)
3. Федеральный закон от 10 января 2002 г. N 1-ФЗ "Об электронной цифровой подписи" (с изменениями от 8 ноября 2007 г.)
4. Федеральный закон от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне" (с изменениями от 2 февраля, 18 декабря 2006 г., 24 июля 2007 г.)
5. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895)
6. Постановление Правительства РФ от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"
7. Приказ Министерства информационных технологий и связи РФ от 9 января 2008 г. N 1 "Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации"

Основная литература

1. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.: - Режим доступа: http://znanium.com/catalog/product/987215
2. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html. — Режим доступа: для авторизир. Пользователей

Дополнительная литература

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 c. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72341.html
2. Фомин, Д. В. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — М. : Московский технический университет связи и информатики, 2015. — 35 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/61737.html.
3. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст :

электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html

4. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 242 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/62945.html

5. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учеб. пособие / Ю.Н. Сычев. — М. : ИНФРА-М, 2019. — 223 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. - Режим доступа: http://znanium.com/catalog/product/979415

6. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере / А. Е. Фаронов. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/52160.html.

7. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: http://www.iprbookshop.ru/77319.html.

6.2. Перечень ресурсов информационно-текоммуникационной сети «Интернет»

1. http://www.eios.dom-rggu.ru/ - электронная информационо-образовательная среда (ЭИОС) филиала РГГУ в г.Домодедово

2. http://www.znanium.com - Электронные учебники электронно-библиотечной системы Znanium

3. Электронно-библиотечная система IPRbooks (ЭБС IPRbooks) - http://www.iprbookshop.ru/

4. Электронная информационно-образовательная среда (ЭИОС) филиала РГГУ в г. Домодедово – http://www.eios.dom-rsuh.ru/

5. Информационно-правовой портал - https://www.garant.ru

Состав современных профессиональных баз данных (БД) и информационно-справочные систем

№п/п	Наименование
1	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины

Реализация учебной дисциплины требует наличия лекционного кабинета со следующим оборудованием:

1. Ноутбук с программным обеспечением Microsoft PowerPoint;
2. Проектор для демонстрации слайдов Microsoft PowerPoint;
3. Экран для демонстрации слайдов Microsoft PowerPoint.

Для преподавания дисциплины необходим доступ к электронной информационно-образовательной среде (ЭИОС) филиала, электронному каталогу библиотеки института, а также оборудование для мультимедийных презентаций.

Программное лицензионное обеспечение дисциплины: Windows 7 Pro, Windows 8,1, Windows 10 Pro, Microsoft office 2010/2013

Освоение дисциплины предполагает использование академической аудитории для проведения лекционных и практических занятий с необходимыми техническими средствами (оборудование для мультимедийных презентаций).

Состав программного обеспечения (ПО) (2022 г.)

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Операционная система тонких клиентов WTware	WTware	Лицензионное
2	Windows server 2008	Microsoft	Лицензионное
3	Microsoft office 2010/2013	Microsoft	Лицензионное
4	Windows 7 Pro	Microsoft	Лицензионное
5	MyTestXPro	MyTestX	Лицензионное
6	Windows server 2012	Microsoft	Лицензионное
7	Windows 8.1	Microsoft	Лицензионное
8	Windows 10 Pro	Microsoft	Лицензионное
9	Dr. Web	Dr. Web	Лицензионное
10	Касперский	Лаборатория Касперского	Свободно распространяемое
11	AutoCAD 2010 Student	Autodesk	Свободно распространяемое
12	Archicad 21 Rus Student	Graphisoft	Свободно распространяемое
13	Adobe Acrobat Reader 9	Adobe Systems	Лицензионное
14	Zoom	Zoom	Лицензионное

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

- письменные задания оформляются увеличенным шрифтом;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

- письменные задания выполняются на компьютере в письменной форме;

- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;

- в форме электронного документа;

- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;

- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;

- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
  - устройством для сканирования и чтения с камерой SARA CE;
  - дисплеем Брайля PAC Mate 20;
  - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
  - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - передвижными, регулируемыми эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Практическое занятие 1. Тема Основы информационной безопасности

ТЕМА: 1.1. Понятие информационной безопасности. Основные составляющие.
Вопросы:

1. Понятие «Информационная безопасность».
2. Место информационной безопасности и Информационной безопасности РФ.
3. Обеспечение информационной безопасности.
4. Обеспечение доступности информации.
5. Обеспечение целостности информации.
6. Обеспечение конфиденциальности информации.

Литература

1. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.: - Режим доступа: http://znanium.com/catalog/product/987215

2. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html. — Режим доступа: для авторизир. Пользователей

3. Фомин, Д. В. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — М. : Московский технический университет связи и информатики, 2015. — 35 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/61737.html

ТЕМА 1.2. Наиболее распространенные угрозы информационной безопасности и ее составляющие
Вопросы

1. Перечислите виды угроз безопасности информации.
2. Каковы источники угроз безопасности информации?
3. Каковы проблемы защиты электронной информации?
4. Что такое компьютерное преступление?
5. Дайте классификацию компьютерным преступлениям.
6. Правовое обеспечение защиты информации.
7. Опишите механизмы преступлений с использованием пластиковых карт.
8. Опишите мошенничество на Интернет-аукционах.
9. Компьютерные вирусы и средства защиты от них.
10. Троянские программы, использование троянских программ для совершения компьютерных преступлений.
11. Что такое информационная атака?
12. Что такое информационная война?
13. Что такое электронный терроризм?

Литература

1. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.: - Режим доступа: http://znanium.com/catalog/product/987215

2. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html. — Режим доступа: для авторизир. Пользователей

3. Фомин, Д. В. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — М. : Московский технический университет связи и информатики, 2015. — 35 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/61737.html

ТЕМА: 2.1. Тема. Законодательный уровень информационной безопасности.
Вопросы

1. Задачи Информационной безопасности общества.
2. Законодательно-правовой уровень обеспечения информационной безопасности
3. Ответственность за нарушение в сфере информационной безопасности
4. Стандарты информационной безопасности

Литература

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 c. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72341.html

2. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html

3. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 242 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/62945.html

4. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html. — Режим доступа: для авторизир. Пользователей

5. Фомин, Д. В. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — М. : Московский технический университет связи и информатики, 2015. — 35 c. —

ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/61737.html

ТЕМА: 2.2. Административный уровень информационной безопасности
Вопросы

1. Цели, задачи и содержание административного уровня.
2. Политика информационной безопасности
3. Содержание политики информационной безопасности фирмы
4. Разработка политики информационной безопасности

Литература

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 c. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72341.html

2. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.: - Режим доступа: http://znanium.com/catalog/product/987215

3. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html. — Режим доступа: для авторизир. Пользователей

4. Фомин, Д. В. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — М. : Московский технический университет связи и информатики, 2015. — 35 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/61737.html

ТЕМА: 2.3. Процедурный уровень информационной безопасности
Вопросы

1. Управление персоналом
2. Поддержание работоспособности
3. Планирование восстановительных работ
4. Физическая защита
5. Реагирование на нарушение безопасного режима

Литература

1. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html

2. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учеб. пособие / Ю.Н. Сычев. — М. : ИНФРА-М, 2019. — 223 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. - Режим доступа: http://znanium.com/catalog/product/979415

3. Фомин, Д. В. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной

безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — М. : Московский технический университет связи и информатики, 2015. — 35 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/61737.html

Практическое занятие 3. Тема Основные характеристики программно-технических мер обеспечение информационной безопасности

Вопросы

- Основные понятия программно-технического уровня информационной безопасности
- Объективные причины, затрудняющие обеспечение надежной защиты
- Основные сервисы безопасности

Тема 3.2. Идентификация и аутентификация

Вопросы

1. Понятие идентификация/аутентификация
2. Причины возможного снижения надежности идентификации
3. Парольная аутентификация
4. Проблемы парольной аутентификации
5. Характеристики идентификации/аутентификации с помощью биометрических данных
6. Каким угрозам подвержена биометрическая аутентификация

Литература

1. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере / А. Е. Фаронов. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/52160.html.

2. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: http://www.iprbookshop.ru/77319.html.

3. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html. — Режим доступа: для авторизир. Пользователей

4. Фомин, Д. В. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — М. : Московский технический университет связи и информатики, 2015. — 35 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/61737.html

Тема Протоколирование и аудит, шифрование, контроль целостности

Вопросы

1. Протоколирование и аудит. Основные понятия.
2. Активный аудит. Основные понятия.
3. Функциональные компоненты и архитектура.
4. Шифрование.

5. Контроль целостности.

Основная литература

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 c. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72341.html

2. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html

3. Фомин, Д. В. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — М. : Московский технический университет связи и информатики, 2015. — 35 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/61737.html

Тема Экранирование, анализ защищенности
Вопросы

1. Понятие межсетевого экранирования
2. Типы межсетевых экранов, краткая характеристика.
3. Технология виртуальных частных сетей (VPN).

Литература

4. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 c. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72341.html

5. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 c. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: http://www.iprbookshop.ru/77319.html.

6. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html. — Режим доступа: для авторизир. Пользователей

Тема Обеспечение высокой доступности
Вопросы

1. Основные понятия:

- заданный уровень доступности
- Эффективности
- Время недоступности

2. Основные меры обеспечения высокой доступности
- Структуризация системы
- Высокая отказоустойчивость (резервирование, тиражирование);
- Обслуживаемость информационной системы.

Литература

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 c. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72341.html

2. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 c. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: http://www.iprbookshop.ru/77319.html.

9.2. Методические рекомендации по выполнению проверочных работ

1. Суть и значение проверочной работы.

Контрольная работа является документом, свидетельствующими об уровне самостоятельной работы и степени овладения студентами программного материала и его умением кратко и доходчиво проанализировать и изложить в письменной форме выбранную тему.

Выполнение работ существенно влияет на самообразование студентов как специалистов в области мировой экономики, так как это является важным видом самостоятельной интеллектуальной деятельности.

2. Цели проверочной работы:

Целью работы являются: развитие интереса студента(ки) к проблемам мировой экономики; умение работать с различными источниками информации; делать правильные выводы и эффективные предложения.

3. Порядок подготовки проверочной работы.

Тема проверочной работы выбирается студентами самостоятельно.

После выбора темы слушателям необходимо составить предварительный список литературы. Весьма полезно использование оперативных материалов конкретных предприятий и организаций, а также иностранных источников.

Готовая работа в напечатанной форме сдается ведущему курс преподавателю.

4. Требования к проверочной работе.

Главный критерий качества работы – полнота и комплексность освещения темы. Каждый раздел работы должен начинаться с соответствующего заголовка по оглавлению с нумерацией каждой страницы. Работа, не отвечающая определенным нормам, к защите не допускается. Небрежно выполненная работа также к защите не допускается.

Работа должна состоять из: оглавления, введения, основных разделов работы, расчетной части (если это курсовая работа), заключения и списка литературных источников.

5. Примерная схема структуры проверочной работы.

Титульный лист

Оглавление - содержание работы с нумерацией страниц.

Введение. Здесь формируются цели и задачи работы, обосновываются актуальность и практическая значимость темы, мотивы выбора. Можно отметить также трудности, встретившиеся при написании работы, характер использованных источников.

Основные разделы работы. Два, три и более разделов, для полноты освещения темы по основным постановочным вопросам. Постановочные вопросы – это вопросы, раскрывающие суть проблемы или темы. Каждый раздел начинается с заголовка, указанного в оглавлении или содержании с порядковым номером раздела.

Заключение. В нем формируются выводы, предложения или рекомендации по совершенствованию мероприятий, касающихся выбранной вами темы.

*Список использованных источников и литературы***.** Здесь перечисляются источники, нормативные акты, официальные статистические сборники и публикации, монографии, статьи, периодические издания и так далее, которые были использованы при выполнении курсовой или проверочной работы (обязательно указывать год и место издания).

П*риложение* включает таблицы, схемы, графики, копии контрактов, соглашений, писем, расчеты и т.д. Причем их наличие значительно повышает ценность работы.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность» реализуется кафедрой математических и естественнонаучных дисциплин филиала РГГУ в г. Домодедово

Цель освоения учебной дисциплины:

- ознакомление обучающихся с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей, и, конечно, методов их применения.

Задачи изучения дисциплины «Информационная безопасность»:

- сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;
- передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;
- сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

Формируемые компетенции, соотнесенные с планируемыми результатами обучения по дисциплине.

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4.3 Использует информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач для достижения профессиональных целей на государственном и иностранном (-ых) языках	*Знать:* стандартные коммуникативные задачи для достижения профессиональных целей на государственном и иностранном (-ых) языках *Уметь:* использовать коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач *Владеть:* навыками использования информационно-коммуникационных технологий при поиске необходимой информации в процессе решения стандартных коммуникативных задач для достижения профессиональных целей на государственном и иностранном (-ых) языках
ПК-2 Способен	ПК-2.3 Вводит в действие регламент процесса	*Знать:* механизм ввода в действие регламента процесса

регламентировать процессы подразделений организации	подразделения организации	подразделения организации *Уметь:* вводить в действие регламент процесса подразделения организации *Владеть:* навыками ввода в действие регламента процесса подразделения организации
	ПК-2.4 Осуществляет контроль выполнения регламента процесса подразделения организации	*Знать:* механизм контроля выполнения регламента процесса подразделения организации *Уметь:* контролировать выполнение регламента процесса подразделения организации *Владеть:* навыками осуществления контроля выполнения регламента процесса подразделения организации

По дисциплине предусмотрена промежуточная аттестация в форме зачета с оценкой
Общая трудоёмкость дисциплины составляет 3 зачётные единицы.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1			
2			
3			
4			