МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

«Основы информационной безопасности»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация Обеспечение информационной безопасности распределенных информационных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____/Чопоров О.Н./

Заведующий кафедрой
Систем информационной
безопасности _____/А.Г. Остапенко/

Руководитель ОПОП _____/А.Г. Остапенко/

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины: обеспечить будущими инженерам, базовые знания и умения в области информационной безопасности для изучения последующих дисциплин

1.2. Задачи освоения дисциплины

знакомство с профессиональной терминологией в области информационной безопасности;

системное знакомство с проблематикой обеспечения информационной безопасности;

знакомство с местом и ролью информационной безопасности в системе национальной безопасности Российской Федерации, основами государственной информационной политики;

знакомство с нормативно-правовой базой в области информационной безопасности;

знакомство с классификацией угроз и уязвимостей информационной безопасности;

знакомство с основными средствами и способами обеспечения информационной безопасности, принципами построения систем защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Основы информационной безопасности» относится к дисциплинам базовой части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Основы информационной безопасности» направлен на формирование следующих компетенций:

ОК-5 – способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

ОПК-6 – способностью применять нормативные правовые акты в своей профессиональной деятельности

ПК-1 – Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОК-5	знать сущность и понятие информации, информационной безопасности и характеристика ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России
	уметь классифицировать и оценивать угрозы информационной безопасности для телекоммуникационных систем
	владеть профессиональной терминологией в области информационной безопасности
ОПК-6	знать нормативно-правовую базу РФ в области информационной безопасности
	уметь осуществлять выбор нормативно-правового акта для решения практических задач
	владеть навыками использования нормативно-правовой базы в области информационной безопасности
ПК-1	знать источники и классификацию угроз информационной безопасности; современные методы и средства обеспечения информационной безопасности
	уметь осуществлять выбор адекватных защитных мер в соответствии с нормативно правовыми актами РФ
	владеть навыками разработки политики безопасности организации

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Основы информационной безопасности» составляет 4 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		4
Аудиторные занятия (всего)	36	36
В том числе:		
Лекции	18	18
Лабораторные работы (ЛР)	18	18
Самостоятельная работа	108	108

Виды промежуточной аттестации – зачет с оценкой	+	+
Общая трудоемкость: академические часы зач.ед.	 144 4	 144 4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Основные понятия и задачи информационной безопасности	Понятие информации, виды информации, классификация информации по режиму доступа, защита информации. Система менеджмента информационной безопасности (СМИБ), активы, угрозы и уязвимости, инцидент информационной безопасности, ущерб, риск, менеджмент риска ИБ, защитные меры. Понятие информационной безопасности и его составляющие. Понятие тайны, виды тайн. Процессный подход в СМИБ (модель PDCA). Связи между процессами модели PDCA.	2	-	18	20
2	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ	Понятие национальной безопасности РФ. Классификация национальных интересов РФ в информационной сфере. Угрозы и источники угроз в информационной сфере РФ. Общая структура государственной системы обеспечения информационной безопасности Российской Федерации. Основные функции и задачи ФСТЭК России. Государственная система обеспечения информационной безопасности. Государственная информационная политика обеспечения информационной безопасности России.	2	4	18	24
3	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности	Виды нормативно-правового и справочного обеспечения в области информационной безопасности. Концептуальные документы в области информационной безопасности. Нормативно-правовые акты Российской Федерации: кодексы, Законы РФ. Основные подзаконные акты в области защиты информации (Указы Президента и постановления Правительства Российской Федерации). Ведомственная нормативная база в области защиты информации: нормативные документы и инструктивные материалы ФСБ РФ и ФСТЭК (Гостехкомиссии) России.	4	4	18	26

4	Угрозы и уязвимости информационной безопасности	Системная классификаций и общий анализ угроз безопасности информации. Предпосылки появления угроз безопасности информации. Основные типы кибератак. Каналы несанкционированного получения информации. Уязвимости информационной безопасности. Методы оценки уязвимостей. Тестирование информационной системы.	2	4	18	24
5	Стандарты информационной безопасности	Общие вопросы стандартизации. История развития стандартов в области информационной безопасности. Критерии безопасности компьютерных систем Министерства обороны США – «Оранжевая книга». Европейские критерии безопасности информационных технологий. Американские Федеральные критерии безопасности информационных технологий. Общие критерии безопасности информационных технологий. Семейство стандартов 27000 системы менеджмента информационной безопасности.	2	-	18	20
6	Методы и средства обеспечения информационной безопасности	Классификация методов и средств защиты данных. Формальные средства защиты. Физические средства защиты: основные решаемые задачи, классификация. Аппаратные средства защиты: отказоустойчивые дисковые массивы, источники бесперебойного питания. Криптографические методы и средства защиты данных: классификация; методы шифрования (замена, перестановка, аналитические преобразования, гаммирование); методы кодирования; методы битовых манипуляций, методы сжатия информации. Потоковые шифры. Симметричные алгоритмы шифрования (DES, ГОСТ 28147-89). Ассиметричные системы шифрования (алгоритм RSA, криптосистема Эль-Гамаля, криптосистемы на основе эллиптических уравнений). Электронная цифровая подпись. Основы криптоанализа. Стеганография. Защита компьютерных систем от вредоносных программ. Защита программных средств от несанкционированного использования и копирования. Методы и средства защиты информации от несанкционированного доступа. Защита информации от несанкционированного доступа в сетях передачи данных.	6	6	18	30
		Итого	**18**	**18**	**108**	**144**

5.2 Перечень лабораторных работ

1. Изучение и анализ ФЗ РФ «Об информации, информационных технологиях и о защите информации», Стратегии национальной безопасности РФ и Доктрины информационной безопасности РФ

2. Изучение и анализ современной нормативной правовой базы в области информационной безопасности.

3. Анализ угроз, уязвимостей информационной безопасности и случаев их реализации

4. Изучение криптографических методов защиты

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОК-5	знать сущность и понятие информации, информационной безопасности и характеристика ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России	знает сущность и понятие информации, информационной безопасности и характеристики ее составляющих; имеет представления о месте и роли информационной безопасности в системе национальной безопасности Российской Федерации, основах государственной информационной политики, стратегии развития информационного общества в России	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	уметь классифицировать и оценивать угрозы информационной безопасности для телекоммуникационных систем	умеет классифицировать и оценивать угрозы информационной безопасности для телекоммуникационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть профессиональной терминологией в области информационной безопасности	владеет профессиональной терминологией в области информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-6	знать нормативно-правовую базу РФ в области информационной безопасности	знает нормативно-правовую базу РФ в области информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь осуществлять выбор нормативно-правового акта для решения практических задач	умеет осуществлять выбор нормативно-правового акта для решения практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками использования нормативно-правовой базы в области информационной безопасности	владеет навыками использования нормативно-правовой базы в области информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-1	знать источники и классификацию угроз информационной безопасности; современные методы и средства обеспечения информационной безопасности	знает источники и классификацию угроз информационной безопасности; имеет представления и современных методах и средствах обеспечения информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь осуществлять выбор адекватных защитных мер в соответствии с нормативно правовыми актами РФ	умеет осуществлять выбор адекватных защитных мер в соответствии с нормативно правовыми актами РФ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками разработки политики безопасности организации	владеет навыками разработки политики безопасности организации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 4 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;
«неудовлетворительно».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОК-5	знать сущность и понятие информации, информационной безопасности и характеристика ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь классифицировать и оценивать угрозы информационной безопасности для телекоммуникационных систем	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть профессиональной терминологией в области информационной безопасности	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-6	знать нормативно-правовую базу РФ в области информационной безопасности	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь осуществлять выбор нормативно-правового акта для решения практических задач	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками использования нормативно-правовой базы в области информационной	Решение прикладных задач в конкретной предметной	Задачи решены в полном объеме и получены	Продемонстрирован верный ход решения всех, но не	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	безопасности	области	верные ответы	получен верный ответ во всех задачах		
ПК-1	знать источники и классификацию угроз информационной безопасности; современные методы и средства обеспечения информационной безопасности	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь осуществлять выбор адекватных защитных мер в соответствии с нормативно правовыми актами РФ	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками разработки политики безопасности организации	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Информация это -

- сведения, поступающие от СМИ
- только документированные сведения о лицах, предметах, фактах, событиях
- **сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления**
- только сведения, содержащиеся в электронных базах данных

2. Информация, зафиксированная на материальном носителе, с реквизитами,позволяющими ее идентифицировать, называется

- достоверной
- конфиденциальной
- **документированной**
- коммерческой тайной

3. Формы защиты интеллектуальной собственности -

- **авторское, патентное право и коммерческая тайна**
- интеллектуальное право и смежные права
- коммерческая и государственная тайна

- гражданское и административное право

4. По доступности информация классифицируется на

- открытую информацию и государственную тайну
- конфиденциальную информацию и информацию свободного доступа
- **информацию с ограниченным доступом и общедоступную информацию**
- виды информации, указанные в остальных пунктах

5. К конфиденциальной информации относятся документы, содержащие

- **государственную тайну**
- законодательные акты
- "ноу-хау"
- сведения о золотом запасе страны

6. Запрещено относить к информации ограниченного доступа

- информацию о чрезвычайных ситуациях
- информацию о деятельности органов государственной власти
- документы открытых архивов и библиотек
- **все, перечисленное в остальных пунктах**

7. К конфиденциальной информации не относится

- коммерческая тайна
- персональные данные о гражданах
- государственная тайна
- **"ноу-хау"**

8. Вопросы информационного обмена регулируются (...) правом

- **гражданским**
- информационным
- конституционным
- уголовным

9. Конфиденциальная информация это

- сведения, составляющие государственную тайну
- сведения о состоянии здоровья высших должностных лиц
- **документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ**
- данные о состоянии преступности в стране

10. Какая информация подлежит защите?

- информация, циркулирующая в системах и сетях связи
- зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
- только информация, составляющая государственные информационные ресурсы
- **любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу**

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Система защиты государственных секретов определяется Законом

- "Об информации, информатизации и защите информации"
- "Об органах ФСБ"
- **"О государственной тайне"**
- "О безопасности"

2. Классификация и виды информационных ресурсов определены

- **Законом "Об информации, информатизации и защите информации"**
- Гражданским кодексом
- Конституцией
- всеми документами, перечисленными в остальных пунктах

3. Формой правовой защиты литературных, художественных и научных произведений является (...) право

- литературное
- художественное
- **авторское**
- патентное

4. Запрещено относить к информации с ограниченным доступом

- **законодательные акты, информацию о чрезвычайных ситуациях и информацию о деятельности органов государственной власти (кроме государственной тайны)**
- только информацию о чрезвычайных ситуациях
- только информацию о деятельности органов государственной власти (кроме государственной тайны)
- документы всех библиотек и архивов

5. К коммерческой тайне могут быть отнесены

- сведения не являющиеся государственными секретами
- сведения, связанные с производством и технологической информацией
- сведения, связанные с управлением и финансами
- **сведения, перечисленные в остальных пунктах**

6. Какой законодательный акт содержит сведения по защите коммерческой тайны?

- Закон "Об авторском праве и смежных правах"
- **Закон "О коммерческой тайне"**
- Патентный закон
- Закон "О правовой охране программ для ЭВМ и баз данных"

7. К информации ограниченного доступа не относится

- государственная тайна
- размер золотого запаса страны
- **персональные данные**
- коммерческая тайна

8. Система защиты государственных секретов

- основывается на Уголовном Кодексе РФ
- регулируется секретными нормативными документами

- определена Законом РФ "О государственной тайне"

- осуществляется в соответствии с п.1-3

9. Документы, содержащие государственную тайну снабжаются грифом

- "секретно"
- "совершенно секретно"
- "особой важности"

- указанным в п.1-3

10. Предельный срок пересмотра ранее установленных грифов секретности составляет

- 5 лет

- 1 год
- 10 лет
- 15 лет

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Программное средство защиты информации

- криптография

- источник бесперебойного питания
- резервное копирование
- дублирование данных

2. Обеспечение достоверности и полноты информации и методов ее обработки

- конфиденциальность

- целостность

- доступность
- целесообразность

3. Как называется документ в программе MS Access?

- таблица

- база данных

- книга
- форма

4. Виды защиты БД

- защита паролем, защита пользователем

- учётная запись группы администратора
- приложение, которое используется для управления базой данных
- группа Users

5. Защита через права доступа заключается

- присвоении каждому пользователю определенного набора прав

- запереть серверы в специальном помещении с ограниченным доступом
- присвоить пароль каждому общедоступному ресурсу
- в наличии преобразователья микрофона

6. Наиболее распространенный криптографический код

- Код Хэмминга

- код Рида-Соломона

- код Морзе
- итеративный код

7. Функция технологии RAID 5

- дисковый массив повышенной производительности с чередованием, без отказоустойчивости
- зарезервирован для массивов, которые применяют код Хемминга
- хранит блок четности на одном физическом диске
- **распределяет информацию о четности равномерно по всем дискам**

8. Какой способ данные, дублируя и размещая их на различных физических носителях (например, на разных дисках)

- Журнал резервного копирования
- **Отказоустойчивые системы**
- Метод резервного копирования
- Шифрование данных

9. Международным стандартным кодом является

- **Unicode**
- CP866
- ASCII
- DOS
- Altair

10. Утилита Setup это - ?

- **утилита входящая в состав BIOS**
- утилита содержащее в себе BIOS
- BIOS не содержит ее
- настройка системы BIOS

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для решения прикладных задач

1. Дайте определение «информация», «защищаемая информация». Как классифицируется информация в зависимости от категории доступа, от порядка ее предоставления или распространения?

2. Дайте определение «защита информации». Что является предметом защиты?

3. Дайте определения: «угроза», «воздействие», «источник угроз», «уязвимость», «ущерб», «риск», «информационный риск».

4. Что такое «инцидент информационной безопасности» и «событие в системе информационной безопасности»?

5. Что представляет собой модель злоумышленника?

6. Что такое «защитная мера»? Какова структура защитных мер? Что относится к базовым защитным мерам?

7. Что представляет собой система обеспечения безопасности? Какие задачи она решает?

8. Дайте определение «информационная безопасность» и перечислите

основные ее составляющие.

9. Перечислите и охарактеризуйте основные виды тайн.

10. Что представляет собой система менеджмента информационной безопасности? Перечислите и охарактеризуйте основные процессы, входящие в модель PDCA.

11. Что такое «политика информационной безопасности»? Перечислите основные ее положения.

12. Что понимается под национальной безопасностью РФ? Что относится к национальным интересам России в информационной сфере? Приведите их классификацию, в соответствии с Доктриной информационной безопасности РФ.

13. Что понимается под информационной безопасностью РФ? Перечислите основные задачи обеспечения информационной безопасности РФ.

14. Перечислите виды угроз информационной безопасности РФ. Что относится к внешним и внутренним источникам угроз информационной безопасности РФ.

15. Что входит в общую структуру государственной системы обеспечения информационной безопасности РФ?

16. Перечислите основные функции и задачи, решаемые ФСТЭК России.

17. Перечислите основные функции и задачи, решаемые ФСБ России в области обеспечения информационной безопасности.

18. Какие задачи решает государственная система обеспечения информационной безопасности?

19. Перечислите основные принципы государственной политики обеспечения информационной безопасности РФ.

20. Перечислите основные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ, определенные в Доктрине информационной безопасности РФ.

21. В чем заключается правовое обеспечение информационной безопасности? Что понимается под нормативно-правовым актом?

22. Опишите структуру нормативно-правового и справочного обеспечения информационной безопасности информационных технологий, охарактеризуйте отдельные компоненты.

23. Какие международные организации занимаются разработкой нормативно-правовых актов в области информационной безопасности.

24. Опишите основные концептуальные документы, определяющие основу защиты информации в России.

25. Перечислите основные федеральные законы РФ, определяющие систему защиты информации в России.

26. Какие вспомогательные нормативные акты регулируют процесс и механизмы исполнения положений и требований к системе обеспечения информационной безопасности государства? Дайте их краткую характеристику.

27. Опишите основные положения закона «О коммерческой тайне».

28. Опишите основные положения закона «О государственной тайне».

29. Опишите основные положения закона «Об электронной подписи».

30. Опишите основные положения закона «О персональных данных».

31. Как классифицируются информационные системы в зависимости от категории и объема обрабатываемых персональных данных?

32. Что относится к угрозам безопасности персональных данных 1-го, 2-го и 3-го типов?

33. Опишите требования к необходимости обеспечения четырех уровней защищенности персональных данных.

34. Перечислите основные руководящие документы Гостехкомиссии России. Дайте их краткую характеристику.

35. Охарактеризуйте 7 классов средств вычислительной техники (СВТ) по уровню защищенности от НСД.

36. Охарактеризуйте 9 классов защищенности автоматизированных систем (АС) от НСД.

37. Перечислите основные нормативно-методические документы ФСТЭК России в области защиты персональных данных. Дайте их краткую характеристику.

38. Перечислите основные руководящие документы ФСТЭК России по защите ключевых систем информационной инфраструктуры.

39. По каким параметрам могут классифицироваться угрозы информационной безопасности? Представьте системную классификацию угроз информационной безопасности и дайте их краткую характеристику.

40. Перечислите основные предпосылки появления угроз информационной безопасности, дайте их краткую характеристику.

41. Что понимается под источником угрозы информационной безопасности? Дайте их краткую характеристику.

42. Перечислите основные типы кибератак. Дайте их краткую характеристику.

43. Опишите основные составляющие модели угроз информационной безопасности.

44. Что такое каналы несанкционированного получения информации? На какие классы и по каким признакам они делятся?

45. По каким признакам классифицируются уязвимости информационной безопасности? Дайте их краткую характеристику.

46. Перечислите и охарактеризуйте основные методы оценки уязвимостей.

47. Какие выделяются категории стандартов по защите информации? Чем отличаются добровольные, регулирующие стандарты и регулятивное использование добровольных стандартов?

48. Перечислите наиболее известные зарубежные и отечественные стандарты в области информационной безопасности?

49. Что такое «Оранжевая книга»? Какие понятия были впервые в ней введены? Что подразумевается под безопасной компьютерной системой?

50. Что такое произвольное и принудительное управление доступом?

Перечислите и охарактеризуйте основные элементы принудительного управления доступом.

51. Опишите основные требования безопасности, предложенные в «Оранжевой книге».

52. Какие классы защищенности были определены в «Оранжевой книге»? Дайте их краткую характеристику.

53. Какие понятия были впервые введены в Европейских критериях безопасности информационных технологий? Опишите основные классы защищенности.

54. Каковы основные особенности Общих критериев безопасности информационных технологий? В чем заключается концепция профиля защиты?

55. Опишите семейство стандартов 27000 системы менеджмента информационной безопасности.

56. По каким критериям классифицируются средства защиты данных? Что такое формальные и неформальные средства защиты?

57. Какие задачи решают, и по каким признакам классифицируются физические средства защиты информации?

58. Перечислите основные разновидности и характерные особенности устройств с идентификационными картами.

59. Перечислите основные методы биометрической идентификации.

60. Что такое отказоустойчивые дисковые массивы (RAID)? Какие выделяют уровни RAID и какие принципы организации заложены в них?

61. Какие выделяют помехи в электросети и какие устройства используются для защиты от них?

62. Криптографические методы и средства защиты данных, основные понятия: криптография, открытый текст, шифрование данных, шифр, ключ, криптоанализ, криптология.

63. Классификация криптографических методов преобразования информации.

64. Методы гаммирования. Потоковые шифры.

65. Федеральный стандарт США на шифрование данных (DES).

66. Отечественный стандарт на шифрование данных.

67. Современные симметричные системы шифрования.

68. Шифрование с открытым ключом, алгоритм RSA.

69. Электронная цифровая подпись

80. Компьютерная стеганография.

71. Вредоносные программы и их классификация.

72. Методы обнаружения и удаления компьютерных вирусов.

73. Программные закладки и методы защиты от них.

74. Принципы построения систем защиты от копирования. Классификация.

75. Методы и средства защиты информации от несанкционированного доступа.

76. Аутентификация пользователей на основе паролей.

77. Аутентификация пользователей на основе модели «рукопожатия».
78. Аутентификация пользователей при удаленном доступе.
79. Защита информации от несанкционированного доступа в сетях.
80. Межсетевые экраны.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет с оценкой проводится по билетам, каждый из которых содержит 3 вопроса. Первый вопрос оценивается на 3 балла, второй – на 4 балла, третий – на 5 баллов. Максимальное количество набранных баллов – 12.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 5 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 5 до 7 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 8 до 9 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 10 до 12 баллов)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основные понятия и задачи информационной безопасности	ОК-5, ОПК-6, ПК -1	Тест, защита реферата
2	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ	ОК-5, ОПК-6, ПК -1	Тест, защита реферата
3	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности	ОК-5, ОПК-6, ПК -1	Тест, защита реферата
4	Угрозы и уязвимости информационной безопасности	ОК-5, ОПК-6, ПК -1	Тест, защита реферата
5	Стандарты информационной безопасности	ОК-5, ОПК-6, ПК -1	Тест, защита реферата
6	Методы и средства обеспечения информационной безопасности	ОК-5, ОПК-6, ПК -1	Тест, защита реферата

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

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи

компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Чопоров, О.Н. Основы информационной безопасности [Электронный ресурс] . - Электрон. текстовые, граф. дан. (0,99 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00.

2. Величко, В.В. Основы инфокоммуникационных технологий : Учеб. пособие / под ред. В. П. Шувалова. - М. : Горячая линия -Телеком, 2009. - 712 с. : ил . - ISBN 978-5-9912-0055-4 : 615-00.

Дополнительная литература:

1. Милославская, Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : Учеб.пособие. - 2-е изд., испр. - М. : Горячая линия -Телеком, 2014. - 214 с. : ил . - (Вопросы управления информационной безопасностью. Кн. 4). - ISBN 978-5-9912-0364-7 : 527-00.

2. Милославская, Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : Учеб. пособие. - М. : Горячая линия -Телеком, 2014. - 170 с. : ил . - (Вопросы управления информационной безопасностью. Кн. 3). - ISBN 978-5-9912-0363-0 : 495-00.

3. Методические указания к практическим занятиям по дисциплине «Основы информационной безопасности» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: О. Н. Чопоров, Н. Н. Корнеева. - Электрон. текстовые, граф. дан. (542 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

4. Методические указания к самостоятельным работам по дисциплине «Основы информационной безопасности» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная

безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. О. Н. Чопоров. - Электрон. текстовые, граф. дан. (348 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

5. Основы информационной безопасности : Учебник / В.А.Минаев, С.В.Скрыль, А.П.Фисун, С.В.Дворянкин. - Воронеж : Воронежский институт МВД России, 2001. - 464 с. - 120.00.

6. Основы управления информационной безопасностью / Учеб. пособие. - 2-е изд., испр. - М. : Горячая линия -Телеком, 2014. - 244 с. - (Вопросы управления информационной безопасностью. Кн. 1). - ISBN 978-5-9912-0361-6 : 529-00.

7. Корт С.С. Теоретические основы защиты информации : учеб. пособие. - М. : Гелиос АРВ, 2004. - 240 с. : ил . - ISBN 5-85438-010-2 : 127-00.

8. Милославская, Н.Г. Управление рисками информационной безопасности : Учеб. пособие. - 2-е изд., испр. - М. : Горячая линия -Телеком, 2014. - 130 с. : ил . - (Вопросы управления информационной безопасностью. Кн. 2). - ISBN 978-5-9912-0362-3 : 489-00.

9. Малюк А.А. Информационная безопасность : концептуальные и методологические основы защиты информации : Учеб. пособие. - М. : Горячая линия -Телеком, 2004. - 280 с. - ISBN 5-93517-197-X : 80-00.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Операционная система, не ниже Windows 7.

Пакет офисных программ, не ниже MS Office 2007.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Для проведения лекций – аудитория с проектором и проекционной доской.

Для проведения лабораторных работ – десять рабочих мест, оборудованных ПЭВМ, с установленным программным обеспечением: Windows 7, MS Office 2007.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Основы информационной безопасности» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не

нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.