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 построения защищенных компьютерных сетей»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация Безопасность распределенных компьютерных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ /В.Н. Деревянко/

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

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Целидисциплины

Целью дисциплины является обучение принципам построения информационных систем (компьютерных сетей) в защищенном исполнении в соответствии с государственными требованиями о защите различных категорий конфиденциальной информации и требованиями к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации защищаемых информационных систем.

1.2.Задачиосвоениядисциплины

Задачами освоения дисциплины являются:

- изучение государственных требований о защите различных категорий конфиденциальной информации;
- изучение требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации защищаемых информационных систем;
- изучение мер и средств защиты информации в информационных системах (компьютерных сетях).

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Основыпостроениязащищенныхкомпьютерныхсетей»относитсякдисциплинамбазовойчастиблокаБ1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Основыпостроениязащищенныхкомпьютерныхсетей»направленаформированиеследующихкомпетенций:

ПК-4-способностьюпроводитьанализиучаствоватьвразработкематематическихмоделейбезопасностикомпьютерныхсистем

ПК-11-способностьюучаствоватьвпроведенииэкспериментально-исследовательскихработприпроведенииисертификациисредствзащитыинформациивкомпьютерныхсистемахпотребованиямбезопасностиинформации

ПСК-3.1-способностьюиспользоватьсовременныекритериииистандартыдляанализабезопасностираспределенныхкомпьютерныхсистем

ПСК-3.2-способностьюанализироватьзащитуинформациивраспределенныхкомпьютерныхсистемах,проводитьмониторинг,аудитиконтрольныепроверкиработоспособностиизащищенностираспределенныхкомпьютерныхсистем

ПСК-3.5-способностьюучаствоватьвформировании,реализацииконтролеэффективностиполитикиинформационнойбезопасностираспределенныхкомпьютерныхсистем

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
ПК-4	Знать модели безопасности компьютерных систем
	Уметь адаптировать модели безопасности компьютерных систем в соответствии с требованиями о защите

	информации
	Владеть методами и средствами реализации модели безопасности компьютерных систем в соответствии с требованиями о защите информации
ПК-11	Знать требования к различным видам, классам и типам средств защиты информации
	Уметь определять виды, классы и типы средств защиты информации
	Владеть методами и средствами проверки функциональности средств защиты информации
ПСК-3.1	Знать требования по аттестации на соответствие требованиям по безопасности информации
	Уметь составлять программу и методики аттестационных испытаний
	Владеть методами и средствами проведения аттестационных испытаний
ПСК-3.2	Знать требования о защите информации
	Уметь определять категорию защищаемой информации или класс защищаемой информационной системы
	Владеть методикой формирования дополненного уточненного адаптированного базового набора мер защиты информации
ПСК-3.5	Знать структуру и основные положения политикиинформационнойбезопасностираспределенных компьютерныхсистем
	Уметь формировать и реализовывать политикуинформационнойбезопасностираспределенных компьютерныхсистем
	Владеть методами контроля эффективности политики информационной безопасности распределенных компьютерных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Основыпостроениязащищенныхкомпьютерныхсетей»составляет3з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы	Всегочасов	Семестры
		9
Аудиторныезанятия (всего)	72	72
В томчисле:		
Лекции	36	36
Лабораторныеработы (ЛР)	36	36

Самостоятельнаяработа	36	36
Видыпромежуточнойаттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Лицензирование и сертификация в сфере защиты информации	Лицензирование отдельных видов деятельности. Лицензирование деятельности, связанной с использованием сведений, составляющих государственную тайну. Лицензировании деятельности по технической защите конфиденциальной информации. Лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации. Лицензирование деятельности, связанной с шифрованием.Техническое регулирование. Сертификация по требованиям безопасности информации. Система сертификации средств защиты информации по требованиям безопасности информации. Система сертификации средств криптографической защиты информации.	6	6	6	18
2	Требования об обеспечении безопасности персональных данных	Определение уровня защищенности персональных данных. Оценка защищенности информационной системы персональных данных. Формирование модели угроз безопасности персональных данных и модели нарушителя. Определение состава мер и средств, применяемых для обеспечения безопасности персональных данных	6	6	6	18
3	Требования о защите информации, содержащейся в государственных информационных системах	Определение класса защищенности информационной системы. Требования к организации защиты информации,содержащейся в информационной системе. Требования к мерам защиты информации, содержащейсяв информационной системе. Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы	6	6	6	18
4	Требования об обеспечении безопасности значимых объектов критической информационной инфраструктуры	Категорирование объектов критической информационной инфраструктуры. Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования. Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации	6	6	6	18
5	Порядок создания, развития ввода в эксплуатацию, эксплуатации и вывода из эксплуатации защищаемых	Требования к порядку создания системы. Требования к порядку ввода системы в эксплуатацию. Требования к порядку развития системы. Требования к порядку эксплуатации системы. Требования к порядку вывода системы	6	6	6	18

	информационных систем	из эксплуатации и дальнейшего хранения содержащейсяв ее базах данных информации				
6	Аттестация информационных систем по требованиям безопасности информации	Аттестации объектов информатизации по требованиям безопасности информации. Участники системы аттестации, их права и обязанности. Программа и методики аттестационных испытаний	6	6	6	18
		Итого	**36**	**36**	**36**	**108**

5.2Переченьлабораторныхработ

1. Формирование требований к функциональности средств защиты информации в соответствии с классом и типом.
2. Определение уровня защищенности персональных данных.
3. Определение класса государственной информационной системы.
4. Формирование модели угроз безопасности информации.
5. Формирование модели нарушителя.
6. Формирование дополненного уточненного адаптированного базового набора мер защиты информации.
7. Выбор средств защиты информации, реализующих меры защиты информации.
8. Составление программы и методик аттестационных испытаний.

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплинынепредусматриваетвыполнениекурсовогопроекта(работы)иликонтрольнойработы.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения, характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-4	Знать модели безопасности компьютерных систем	Знание видов и содержания моделей безопасности компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь адаптировать модели безопасности компьютерных систем в	Умение адаптировать модели безопасности компьютерных систем в соответствии с требованиями о защите информации различных категорий, а также	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	соответствии с требованиями о защите информации	структурными и функциональными характеристиками информационных систем		
	Владеть методами и средствами реализации модели безопасности компьютерных систем в соответствии с требованиями о защите информации	Владение методами и средствами, с помощью которых возможна реализация модели безопасности компьютерных систем в соответствии с требованиями о защите информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-11	Знать требования к различным видам, классам и типам средств защиты информации	Знание требований к различным видам, классам и типам средств защиты информации, в том числе криптографичексой	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь определять виды, классы и типы средств защиты информации	Умение определять виды, классы и типы средств защиты информации применительно к решаемым задачам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть методами и средствами проверки функциональност и средств защиты информации	Владение методами и программными средствами проверки функциональности средств защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК-3.1	Знать требования по аттестации на соответствие требованиям по безопасности информации	Знание требований по аттестации информационных систем на соответствие требованиям по безопасности информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь составлять программу и методики аттестационных испытаний	Умение составлять программу и методики аттестационных испытаний с учетом требований о защите информации, а также в соответствии со структурными и функциональными характеристиками информационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть методами и средствами	Способность проводить аттестационные	Выполнение работ в срок,	Невыполнение работ в срок, предусмотренный

	проведения аттестационных испытаний	испытания информационных систем по программе и методикам аттестационных испытаний	предусмотренный в рабочих программах	в рабочих программах
ПСК-3.2	Знать требования о защите информации	Знание требования о защите персональных данных, а также информации, обрабатываемой в государственных информационных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь определять категорию защищаемой информации или класс защищаемой информационной системы	Умение определять категорию защищаемой информации или класс защищаемой информационной системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть методикой формирования дополненного уточненного адаптированного базового набора мер защиты информации	Способность формировать дополненный уточненный адаптированный базовый набор мер защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК-3.5	Знать структуру и основные положения политики информационной безопасности распределенных компьютерных систем	Знание структуры и основных положений политики информационной безопасности распределенных компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь формировать и реализовывать политику информационной безопасности распределенных компьютерных систем	Умение формировать и реализовывать политику информационной безопасности распределенных компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть методами контроля эффективности политики информационной безопасности	Способность оценить эффективность релизации политики информационной безопасности в распределенной компьютерной системе	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	распределенных компьютерных систем			

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв9семестредля очнойформыобученияподвухбалльнойсистеме:

«зачтено»

«незачтено»

Компе-тенция	Результатыобучения, характеризующие сформированностькомпетенции	Критерии оценивания	Зачтено	Незачтено
ПК-4	Знать модели безопасности компьютерных систем	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	Уметь адаптировать модели безопасности компьютерных систем в соответствии с требованиями о защите информации	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	Владеть методами и средствами реализации модели безопасности компьютерных систем в соответствии с требованиями о защите информации	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
ПК-11	Знать требования к различным видам, классам и типам средств защиты информации	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	Уметь определять виды, классы и типы средств защиты информации	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	Владеть методами и средствами	Решение прикладных задач в конкретной	Продемонстрирова н верный ход решения	Задачинерешены

	проверки функциональности средств защиты информации	предметной области	в большинстве задач	
ПСК-3.1	Знать требования по аттестации на соответствие требованиям по безопасности информации	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	Уметь составлять программу и методики аттестационных испытаний	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	Владеть методами и средствами проведения аттестационных испытаний	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
ПСК-3.2	Знать требования о защите информации	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	Уметь определять категорию защищаемой информации или класс защищаемой информационной системы	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	Владеть методикой формирования дополненного уточненного адаптированного базового набора мер защиты информации	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
ПСК-3.5	Знать структуру и основные положения политики информационной безопасности распределенных компьютерных систем	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%

	Уметь формировать и реализовывать политику информационной безопасности распределенных компьютерных систем	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	Владеть методами контроля эффективности политики информационной безопасности распределенных компьютерных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилиныематериалы,необходимыедляоценкизнаний,умений,навыкови(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1. К нормативным правовым актам, регулирующим вопросы ТЗИ, не относится:

А) Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Б) Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ «О ПДн».

В) Федеральный закон Российской Федерации от 06.04.2011 г. №63-ФЗ «Об электронной подписи».

Г) Федеральный закон Российской Федерации от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности».

2. ТЗИ – это:

А) Состояние защищенности объекта информатизации, при котором обеспечивается безопасность информации и автоматизированных средств ее обработки.

Б) Деятельность, направленная на обеспечение некриптографическими методами безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

В) Состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность.

Г) Проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

3. Неверным является утверждение:

А) Участниками сертификации средств защиты информации (далее – СЗИ) являются федеральный орган по сертификации, центральный орган системы сертификации, органы по сертификации СЗИ, испытательные лаборатории, изготовители.

Б) Обязательной сертификации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров.

В) В настоящее время действуют четыре системы сертификации СЗИ: Минобороны России, СВР России, ФСБ России, ФСТЭК России.

Г) Основными схемами проведения сертификации СЗИ являются: проведение испытаний единичных образцов СЗИ на соответствие требованиям по ЗИ и проведение типовых испытаний образцов СЗИ на соответствие требованиям по ЗИ и последующий инспекционный контроль за стабильностью характеристик сертифицированных СЗИ, определяющих выполнение этих требований.

4. К числу документов, определяющих направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности ПДн при их обработке в ИСПДн, не относится:

А) Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации».

Б) Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О ПДн» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

В) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите ПДн при их обработке в ИСПДн».

Г) Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИС ПДн».

5. Неверным является утверждение:

А) Для выполнения работ по обеспечению безопасности ПДн при их обработке в ИСПДн в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

Б) Меры по обеспечению безопасности ПДн реализуются в рамках системы защиты ПДн и должны быть направлены на нейтрализацию всех возможных угроз безопасности ПДн.

В) Меры по обеспечению безопасности ПДн реализуются в том числе

посредством применения в ИСПДн СЗИ, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда, применение таких средств необходимо для нейтрализации актуальных угроз безопасности ПДн.

Г) Оценка эффективности реализованных в рамках системы защиты ПДн мер по обеспечению безопасности ПДн проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации, не реже одного раза в 3 года.

6. Безопасность информации – это:

А) Порядок и правила применения определенных принципов и СЗИ.

Б) Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

В) Состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Г) Степень соответствия результатов защиты информации цели защиты информации.

7. Угроза безопасности информации – это:

А) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Б) Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

В) Свойство информационной системы, обусловливающее возможность нарушения безопасности обрабатываемой в ней информации.

Г) Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

8. Уязвимость – это:

А) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Б) Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

В) Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Г) Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

9. Доступность информации – это:

А) Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

Б) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

В) Состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Г) Состояние информации, при котором обеспечиваются идентификация и регистрация действий с ней.

10. При оценке опасности угрозы в явном виде не учитывается:

А) Исходная или проектируемая защищенность информационной системы.

Б) Вид источника угрозы.

В) Вероятность или возможность реализации угрозы.

Г) Ущерб от реализации угрозы.

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

11. В состав объектов информатизации не входят:

А) Информационные ресурсы.

Б) Средства и системы обработки информации, используемые в соответствии с заданной информационной технологией, и средства их обеспечения.

В) Помещения или объекты (здания, сооружения, технические средства), в которых установлены средства и системы обработки информации.

Г) Административный, технический и обслуживающий персонал.

12. Внутренний потенциальный нарушитель, который имеет доступ к СЗИ и протоколирования и к части ключевых элементов ИСПДн, относится к:

А) К четвертой категории – зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

Б) К пятой категории – зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

В) К шестой категории – зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Г) К седьмой категории – программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

13. Сетевой атакой, цель которой заключается в выявлении работающих в сети служб, открытых портов, активных сетевых сервисов, используемых протоколов, является:

А) Анализ сетевого трафика.

Б) Сканирование сети.

В) Подмена доверенного объекта сети.

Г) Атака «отказ в обслуживании».

14. Сетевой атакой, цель которой заключается в создании таких условий, при которых легитимные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён, является:

А) Анализ сетевого трафика.

Б) Сканирование сети.

В) Подмена доверенного объекта сети.

Г) Атака «отказ в обслуживании».

15. Неверным является утверждение:

А) Программное (программно-математическое) воздействие – это несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Б) Основными видами вредоносных программ являются: программные закладки, программные вирусы, сетевые черви, другие вредоносные программы, предназначенные для осуществления НСД.

В) Программная закладка – это исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.

Г) Сетевой червь – это тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, и осуществлению иного вредоносного воздействия.

16. В состав ГИС не входят:

А) Информация.

Б) Информационные технологии, обеспечивающие обработку информации.

В) Технические средства, обеспечивающие обработку информации.

Г) Сотрудники оператора ГИС.

17. Уровень исходной (проектной) защищенности ИСПДн только снижает:

А) Использование архитектуры «тонкого клиента», наличие подключений к ИСОП, применение многопользовательского режима обработки информации.

Б) Использование архитектуры с удаленным доступом пользователей, расположение технических средств в пределах одной КЗ, применение однопользовательского режима обработки информации.

В) Использование файл-серверной архитектуры, применение технологии беспроводного доступа, применение многопользовательского режима обработки информации.

Г) Использование архитектуры «тонкого клиента», наличие подключений к ИСОП, применение технологий виртуализации.

18. Угрозы безопасности ПДн 2 типа актуальны для ИСПДн, если для нее:

А) В том числе актуальны угрозы, связанные с наличием НДВ в системном ПО, используемом в ИСПДн.

Б) В том числе актуальны угрозы, связанные с наличием НДВ в прикладном ПО, используемом в ИСПДн.

В) Актуальны угрозы, не связанные с наличием НДВ в системном и прикладном ПО, используемом в ИСПДн.

Г) Актуальны угрозы, не связанные с наличием НСД в системном и прикладном ПО, используемом в ИСПДн.

19. К основным угрозам НСД нельзя отнести:

А) Угрозы утечки информации по техническим каналам.

Б) Угрозы проникновения в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения).

В) Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных.

Г) Угрозы внедрения вредоносных программ (программно-математического воздействия).

20. Достаточность и обоснованность запланированных мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн определяет:

А) Оператор.

Б) Роскомнадзор.

В) ФСТЭК России.

Г) ФСБ России.

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

21. Набор мер по обеспечению безопасности ПДн при их обработке в ИСПДн, соответствующий структурно-функциональным характеристикам, информационным технологиям, особенностям функционирования ИСПДн, формируется в результате:

А) Определения базового набора мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

Б) Адаптации базового набора мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

В) Уточнения адаптированного набора мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

Г) Дополнения уточненного адаптированного набора мер по

обеспечению безопасности ПДн при их обработке в ИСПДн.

22. Неверным является утверждение:

А) При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности ПДн.

Б) С учетом экономической целесообразности могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности ПДн.

В) Использование в ИСПДн новых информационных технологий, для которых не определены меры обеспечения их безопасности, не допускается.

Г) В ходе разработки системы защиты ПДн должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности ПДн.

23. Установка и (или) запуск только разрешенного к использованию в ИСПДн ПО или исключение возможности установки и (или) запуска запрещенного к использованию в ИСПДн ПО обеспечиваются:

А) Идентификацией и аутентификацией субъектов доступа и объектов доступа.

Б) Управлением доступа субъектов доступа к объектам доступа.

В) Антивирусной защитой.

Г) Ограничениями программной среды.

24. Обнаружение действий в ИСПДн, направленных на НСД к информации, специальные воздействия на ИСПДн и (или) ПДн в целях добывания, уничтожения, искажения и блокирования доступа к ПДн, а также реагирование на эти действия обеспечиваются:

А) Антивирусной защитой.

Б) Обнаружением (предотвращением) вторжений.

В) Ограничениями программной среды.

Г) Идентификацией и аутентификацией субъектов доступа и объектов доступа.

25. В ГИС 2 класса защищенности ПДн минимально допустимым является применение:

А) СЗИ не ниже 4 класса, а также СВТ не ниже 5 класса.

Б) СЗИ не ниже 5 класса, а также СВТ не ниже 5 класса.

В) СЗИ не ниже 6 класса, а также СВТ не ниже 5 класса.

Г) СЗИ не ниже 6 класса, а также СВТ не ниже 6 класса.

26. К числу документов, которые операторы, являющиеся государственными или муниципальными органами, должны разработать не относится:

А) Правила обработки ПДн.

Б) Правила рассмотрения запросов субъектов ПДн или их представителей.

В) Порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка ПДн.

Г) Правила осуществления внешнего контроля и проверок соответствия обработки ПДн требованиям к защите ПДн.

27. Неверным является утверждение:

А) Операторы, являющиеся государственными (муниципальными) органами, назначают ответственного за организацию обработки ПДн в государственном (муниципальном) органе из числа государственных (муниципальных) служащих данного органа.

Б) Документы, регламентирующие обработку и обеспечение безопасности ПДн, утверждаются ответственным за организацию обработки ПДн в государственном (муниципальном) органе.

В) Документы, определяющие политику в отношении обработки ПДн, подлежат опубликованию на официальном сайте государственного (муниципального) органа в течение 10 дней после их утверждения.

Г) Операторы, являющиеся государственными (муниципальными) органами, осуществляют ознакомление служащих государственного (муниципального) органа, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн.

28. Неверным является утверждение:

А) Аттестация информационной системы организуется обладателем информации (заказчиком) или оператором и включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие системы защиты информации информационной системы требованиям о защите информации.

Б) Проведение аттестационных испытаний информационной системы должностными лицами, осуществляющими проектирование и (или) внедрение системы защиты информации информационной системы, не допускается.

В) Допускается аттестация информационной системы на основе результатов аттестационных испытаний выделенного набора сегментов информационной системы, реализующих полную технологию обработки информации.

Г) Сегмент считается соответствующим сегменту информационной системы, в отношении которого были проведены аттестационные испытания, если для указанных сегментов установлены одинаковые классы защищенности.

29. Предварительные испытания системы защиты информации информационной системы реализуются на этапе:

А) Разработки системы защиты информации информационной системы

Б) Внедрения системы защиты информации информационной системы.

В) Аттестации информационной системы и ввода ее в действие.

Г) Обеспечения защиты информации в ходе эксплуатации аттестованной информационной системы.

30. Неверным является утверждение:

А) Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

Б) Результаты классификации информационной системы оформляются актом классификации.

В) Формирование требований к защите информации, содержащейся в информационной системе, осуществляется организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации, осуществляющей проектирование системы защиты информации информационной системы.

Г) При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

1) Цели и задачи ТЗИ.
2) Объекты информатизации: классификация и характеристика.
3) Основы лицензирования деятельности по ТЗКИ и (или) деятельности по разработке и производству средств защиты информации.
4) Система сертификации средств защиты информации.
5) Порядок разработки, согласования и утверждения планов проведения мероприятий по ТЗКИ.
6) Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций.
7) Классификация ТКУИ.
8) Классификация и характеристики угроз безопасности информации, связанных с НСД.
9) Требования по защите информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.
10) Требования по защите акустической речевой информации.
11) Требования по защите информации от НСД.
12) Стадии и этапы создания системы защиты информации

ограниченного доступа.

13) Способы и средства ТЗКИ от утечки по техническим каналам.

14) Общая характеристика и классификация мер и средств защиты информации от НСД.

15) Основные задачи контроля состояния ТЗКИ.

16) Методы и средства контроля защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.

17) Методы и средства контроля защищенности акустической речевой информации.

18) Методы и средства контроля защищенности информации от НСД.

19) Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.

20) Порядок сертификации продукции, используемой в целях защиты конфиденциальной информации.

21) Порядок организации обработки персональных данных.

22) Порядок обеспечения безопасности персональных данных при из обработке, осуществляемой без использования средств автоматизации.

23) Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

Непредусмотреноучебнымпланом

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

Зачет проводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопрсвтестеоценивается1баллом,задачаоценивается в10баллов(5балловверноерешениеи5балловзаверныйответ).Максимальноеколичествонабранныхбаллов–20.

1.Оценка«Не зачтено»ставитсявслучае,еслистудентнабралменее6баллов.

2.Оценка«Зачтено»ставитсявслучае,еслистудентнабралот6до20баллов.

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочногосредства
1	Лицензирование и сертификация в сфере защиты информации	ПК-4, ПК-11, ПСК -3.1, ПСК-3.2, ПСК -3.5	Тест, контрольная работа, защита лабораторных работ, защита реферата,
2	Требования об обеспечении безопасности персональных данных	ПК-4, ПК-11, ПСК -3.1, ПСК-3.2, ПСК -3.5	Тест, контрольная работа, защита лабораторных работ, защита реферата
3	Требования о защите информации, содержащейся в государственных информационных системах	ПК-4, ПК-11, ПСК -3.1, ПСК-3.2, ПСК -3.5	Тест, контрольная работа, защита лабораторных работ, защита реферата
4	Требования об обеспечении	ПК-4, ПК-11,	Тест, контрольная работа,

	безопасности значимых объектов критической информационной инфраструктуры	ПСК -3.1, ПСК-3.2, ПСК -3.5	защита лабораторных работ, защита реферата
5	Порядок создания, развития ввода в эксплуатацию, эксплуатации и вывода из эксплуатации защищаемых информационных систем	ПК-4, ПК-11, ПСК -3.1, ПСК-3.2, ПСК -3.5	Тест, контрольная работа, защита лабораторных работ, защита реферата
6	Аттестация информационных систем по требованиям безопасности информации	ПК-4, ПК-11, ПСК -3.1, ПСК-3.2, ПСК -3.5	Тест, контрольная работа, защита лабораторных работ, защита реферата

7.3.Методическиематериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатором,ивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении промежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценки припроведениипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература:

1. Деревянко В.Н. Безопасность сетей ЭВМ [Электронный ресурс]: Учеб.пособие / В. Н. Деревянко. - Электрон.текстовые, граф. дан. (7,31 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 30-00.

2. Попов Е. А. Компьютерные сети [Электронный ресурс]: Учеб.пособие / Е. А. Попов, В. Н. Деревянко. - Электрон.текстовые, граф. дан. (2,97 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00.

3. Эпидемии в телекоммуникационных сетях [Текст] / Остапенко Александр Григорьевич [и др.]; под ред. Д. А. Новикова. - Москва: Горячая линия - Телеком, 2018. - 282 с.: ил. - (Теория сетевых войн. № 1). - Библиогр.: с.

231-245 (244 назв.). - ISBN 978-5-9912-0682-2: 736-00.

Дополнительная литература:

1. Нестеровский И.П. Основы безопасности Российской Федерации [Электронный ресурс]: учеб.пособие / И. П. Нестеровский. - Электрон.текстовые, граф. дан. (384 Кб). - Воронеж: ВГТУ, 2005. - 1 файл. - 30-00.

2. Атакуемые взвешенные сети [Текст] / Остапенко Александр Григорьевич [и др.]; под ред. Д. А. Новикова. - Москва: Горячая линия - Телеком, 2018. - 247 с.: ил. - (Теория сетевых войн. № 2). - Библиогр.: с. 201-213 (214 назв.). - ISBN 978-5-9912-0684-6: 708-00.

3. Социальные сети и деструктивный контент [Текст] / Остапенко Александр Григорьевич [и др.]; под ред. Д. А. Новикова. - Москва: Горячая линия - Телеком, 2018. - 274 с.: ил. - (Теория сетевых войн. № 3). - Библиогр.: с. 224-239 (278 назв.). - ISBN 978-5-9912-0686-0: 719-00.

8.2Переченьинформационныхтехнологий,используемыхприосуществлениииобразовательногопроцессаподисциплине,включаяпереченьлицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

1) Банк данных угроз безопасности информации – URL: http://bdu.fstec.ru.

2) Информационно-правовая система «Законодательство России» // Официальный интернет-портал правовой информации – URL: http://pravo.gov.ru/proxy/ips.

3) Каталог стандартов // Официальный сайт Росстандарта – URL: http://www.gost.ru/wps/portal/pages.CatalogOfStandarts.

4) Официальный сайт ФСТЭК России – URL: http://fstec.ru.

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

Компьютерных класс с количеством персональных компьютеров из расчета 1 персональный компьютер на 2 обучающихся.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Основыпостроениязащищенныхкомпьютерныхсетей»читаютсялекции,проводятсялабораторныеработы.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяналиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоответствиисметодиками,приведеннымивуказанияхквыполнениюработ.

Видучебныхзаня	Деятельностьстудента

тий	
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.
Лабораторнаяработа	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.
Самостоятельнаяработа	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 промежуточнойаттестации.
Подготовка к промежуточнойаттестации	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 три дня эффективнее всего использовать для повторения и систематизации материала.