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

«Правовые основы обеспечения компьютерной безопасности»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2016

Автор программы _____ /Л.В. Паринова/

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

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Целидисциплины

Формирование профессиональных навыков, связанных со структурой правового обеспечения информационной безопасности и соответствующего законодательства в области информации, информационных технологий и защиты информации, персональных данных, интеллектуальной собственности, государственной тайны, электронной цифровой подписи, технического регулирования; понятий, связанных с вопросами ответственности за правонарушения в области информационной безопасности, а также механизмами защиты прав и законных интересов субъектов информационной сферы; создание представления о применении организационных и правовых методов обеспечения информационной безопасности в профессиональной деятельности и путях совершенствования системы обеспечения информационной безопасности; к осуществлению контроля эффективности реализации политики информационной безопасности.

1.2.Задачиосвоениядисциплины

Приобретение навыков работы с нормативной информацией в сфере защиты информации; развитие логического мышления, навыков исследования явлений и процессов, связанных с предметной деятельностью; формирование навыков самостоятельной работы, организации исследовательской работы.

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Правовыеосновыобеспечениякомпьютернойбезопасности »относитсякдисциплинамбазовойчастиблокаБ1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Правовыеосновыобеспечениякомпьютернойбезопасности»направленаформированиеследующихкомпетенций:

ОК-4-способностьюиспользоватьосновыправовыхзнанийвразличныхсферахдеятельности

ОК-6-способностьюработатьвколлективе,толерантновоспринимаясоциальные,культурныеиныеразличия

ОК-8-способностьюксамоорганизацииисамообразованию

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
ОК-4	Знать, какие права и обязанности приобретают субъекты, осуществляющие деятельность в информационной сфере, какими правовыми и техническими средствами они могут или должны защищать эти права; какое содействие реализации общественных и государственных интересов они могут оказать для обеспечения информационной безопасности;

	Уметьзащищать свои права на информацию, защищать информацию, том числе обеспечивать ее конфиденциальность, не нарушать права на информацию иных субъектов, содействовать нераспространению запрещенной законом информации;
	Владетьнавыками эффективной работы с электронными базами правовой информации, анализа нормативных правовых актов
ОК-6	Знатьосновные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
	Уметьприменять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
	Владетьнавыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности; методами организации и управления деятельностью служб защиты информации на предприятии;
ОК-8	знатьорганизацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации
	уметь пользоваться нормативными документами по противодействию технической разведке;
	владеть методами формирования требований по защите информации

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Правовыеосновыобеспечениякомпью тернойбезопасности»составляет4з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы	Всегочасов	Семестры
		4
Аудиторныезанятия (всего)	54	54
В томчисле:		

Лекции	36	36
Практическиезанятия (ПЗ)	18	18
Самостоятельнаяработа	90	90
Виды промежуточной аттестации - зачет с оценкой	+	+
Общая трудоемкость: академические часы зач.ед.	 144 4	 144 4

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Практ зан.	СРС	Всего, час
1	Место информационной безопасности в системе информационного права	Органы законодательства, регламентирующие деятельность по информационной безопасности. Структура органов власти по защите информации в Российской Федерации. Совет Безопасности Российской. Федерации. Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации. Федеральная служба безопасности Российской Федерации (ФСБ). Федеральная Служба по техническому и экспортному контролю РФ (ФСТЭК РФ).	6	2	14	22
2	Виды тайн и их правовая защита	Понятие и виды тайн. Виды тайн, охраняемых законом Российской Федерации.	6	2	14	22
3	Правовой режим защиты информации конфиденциального характера	Законодательство Российской Федерации в области защиты конфиденциальной информации. Виды конфиденциальной информации по законодательству Российской Федерации. Отнесение сведений к конфиденциальной информации.	6	2	14	22
4	Институт правовой защиты коммерческой тайны	Нормативно-правовые акты, обеспечивающие возможность защиты коммерческой тайны. Взаимодействие с государственными регуляторами.	6	4	16	26
5	Институт правовой защиты персональных данных	Регуляторы в области защиты ПДн. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Требования к защите персональных данных при их обработке в информационных системах персональных данных.	6	4	16	26
6	Международное законодательство в области обеспечения информационной безопасности	Принципы правового регулирования вопросов обеспечения информационной безопасности и ЗИ в США, Франции, Великобритании, ФРГ и других государствах. Краткая характеристика основных законодательноправовых документов в области ЗИ, действующих в указанных государствах.	6	4	16	26
		Итого	**36**	**18**	**90**	**144**

5.2Переченьлабораторныхработ

Непредусмотреноучебнымпланом

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
ОК-4	Знать, какие права и обязанности приобретают субъекты, осуществляющие деятельность в информационной сфере, какими правовыми и техническими средствами они могут или должны защищать эти права; какое содействие реализации общественных и государственных интересов они могут оказать для обеспечения информационной безопасности;	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь защищать свои права на информацию, защищать информацию, том числе обеспечивать ее конфиденциальность, не нарушать права на информацию иных субъектов, содействовать нераспространению запрещенной законом информации;	Решениестандартныхпрактическихзадач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками эффективной работы с электронными базами правовой информации, анализа нормативных правовых актов	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОК-6	Знать основные нормативные правовые	Тест	Выполнение работ в срок,	Невыполнение работ в срок,

	акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;		предусмотренный в рабочих программах	предусмотренный в рабочих программах
	Уметь применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;	Решениестандартныхпрактическихзадач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности; методами организации и управления деятельностью служб защиты информации на предприятии;	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОК-8	знать организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь пользоваться нормативными документами по противодействию технической разведке;	Решениестандартныхпрактическихзадач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методами формирования требований по защите	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в	Невыполнение работ в срок, предусмотренный

	информации		рабочих программах	в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв4семестредля очнойформыобученияпочетырехбалльнойсистеме:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОК-4	Знать, какие права и обязанности приобретают субъекты, осуществляющие деятельность в информационной сфере, какими правовыми и техническими средствами они могут или должны защищать эти права; какое содействие реализации общественных и государственных интересов они могут оказать для обеспечения информационной безопасности;	Тест	Выполнениетестана 90- 100%	Выполнениетестана 80-90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	Уметь защищать свои права на информацию, защищать информацию, том числе обеспечивать ее конфиденциальность, не нарушать права на информацию иных субъектов, содействовать нераспространению запрещенной законом информации;	Решениестандартныхпрактическихзадач	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	Задачинерешены
	Владеть навыками эффективной работы с электронными базами правовой информации, анализа	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрированверный ход решения всех, но не получен верный ответ во всех	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены

	нормативных правовых актов			задачах		
ОК-6	Знать основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;	Тест	Выполнениетестана 90- 100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	Уметь применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;	Решениестандартныхпрактическихзадач	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	Задачинерешены
	Владеть навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности; методами организации и управления деятельностью служб защиты информации на предприятии;	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	Задачинерешены
ОК-8	знать организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в	Тест	Выполнениетестана 90- 100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов

	области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации					
	уметь пользоваться нормативными документами по противодействию технической разведке;	Решениестандартныхпрактическихзадач	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	Задачинерешены
	владеть методами формирования требований по защите информации	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	Задачинерешены

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

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

Информация в зависимости от порядка ее предоставления или распространения подразделяется на. Отметьте правильный вариант:

свободно распространяемую

предоставляемую по соглашению лиц, участвующих в соответствующих отношениях

подлежащую предоставлению или распространению

распространение которой в РФ ограничивается или запрещается

общедоступную информацию

информацию ограниченного доступа

2. В основу системы классификации АС должны быть положены следующие характеристики объектов и субъектов защиты, а также способов их взаимодействия:

информационные

организационные

технологические

правовые

системные

экономические

3. Какие степени секретности и грифы секретности носителей сведений, установлены законодательством РФ. Отметьте правильный вариант:
для служебного пользования
совершенно секретно
конфиденциально
особой важности
строго конфиденциально
секретно

4. Технологические характеристики АС используемые для классификации, включают в себя:
способ обработки
время циркуляции информации (транзит, хранение)
вид АС (автономная, сеть, стационарная, подвижная)
состав средств вычислительной техники, используемой в процессе обработки информации
категория информации и ее объемы

5. Средства криптографической защиты информации (СКЗИ) это:
совокупность территориально распределенной инфраструктуры программных и технических средств, Администраторов и Операторов Удостоверяющего центра, обеспечивающих деятельность по изготовлению и управлению сертификатами ключей проверки подписей пользователей Удостоверяющего центра и выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи»
уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи
аппаратные, программные или аппаратно-программные средства, осуществляющие криптографические преобразования информации для обеспечения ее безопасности
программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра

6. Защита АС должна обеспечиваться. Отметьте правильные варианты ответа:
на всех технологических этапах обработки информации
во всех режимах работы СВТ, в которых выполняется обработка защищаемой информации
при проведении ремонтных и регламентных работ
в местах хранения информации
на съемных машинных носителях
только при обработке информации СВТ АС

7. Инцидент информационной безопасности это:
идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности
одно или серия нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность нарушения бизнес операций или представляющих угрозу для информационной безопасности
процесс сравнения оценочной величины риска с установленным критерием с целью определения уровня значимости риска
слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами

8. Загрузочные (бутовые) вирусы это:
вирусы, заражающие программы, хранящиеся в системных областях дисков
вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам
вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса
ни один из ответов не является верным

9. Мероприятия по инженерно-технической защите информации от утечки по электромагнитному каналу подразделяются на:
организационные и технические
технические и коммутационные
организационные и объективные
ни один из ответов не является верным

10. Организационно-техническими методами обеспечения информационной безопасности являются. Отметьте правильные варианты ответов:
разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств
развитие защищенных телекоммуникационных систем
создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации
создание систем и средств предотвращения специальных воздействий, вызывающих разрушение, уничтожение, искажение информации
создание систем и средств предотвращения специальных воздействий, вызывающих изменение штатных режимов функционирования систем и средств информатизации и связи
сертификация средств защиты информации
контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности
разработка нормативных методических документов по вопросам обеспечения информационной безопасности

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

Классы защищенности АС от НСД к информации по РД АС подразделяются на группы. Какие?
Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Все пользователи имеют право доступа ко всей информации АС
Вторая группа включает АС, в которых пользователи имеют разные права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности
Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности
Какие показатели, в соответствии с требованиями руководящих документов, должны быть оценены при проведении аттестационных испытаний подсистемы обеспечения целостности автоматизированных систем?
Надежность реализованных на практике функций контроля целостности, неизменность программной среды, выполнение требований по физической охране, работоспособность средств периодического тестирования, наличие и работоспособность технологии восстановления

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

Непредусмотреноучебнымпланом

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

1. Административный уровень информационной безопасности. Политика безопасности.
2. Закон «Об информации, информационных технологиях и защите информации».
3. Основные положения Федерального закона «Об электронной цифровой подписи».
4. Доктрина информационной безопасности Российской федерации.
5. «Критерии оценки доверенных компьютерных систем» как оценочный стандарт.
6. Стандарт ISO/IES 15408 «Критерии оценки безопасности информационных технологий». Краткаяхарактеристика.
7. Оценочныестандарты РФ.
8. Государственная тайна как особый вид защищаемой информации.

9. Система защиты государственной тайны.
10. Засекречивание информации. Организационные и технические способы защиты государственной тайны.
11. Коммерческая тайна.
12. Служебная тайна. Профессиональные тайны.
13. Процессуальные тайны.
14. Персональные данные.
15. Неправомерный допуск к компьютерной информации.
16. Создание, использование и распространение вредоносных программ для ЭВМ.
17. **Криминалистическая характеристика компьютерных преступлений.**

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоцениваетсяв10баллов(5балловверноерешениеи5балловзаверныйответ).Максимальноеколичествонабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее6баллов.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот6до10баллов

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочногосредства
1	Место информационной безопасности в системе информационного права	ОК-4, ОК-6, ОК-8	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Виды тайн и их правовая защита	ОК-4, ОК-6, ОК-8	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Правовой режим защиты информации конфиденциального	ОК-4, ОК-6, ОК-8	Тест, контрольная работа, защита лабораторных

	характера		работ, защита реферата, требования к курсовому проекту….
4	Институт правовой защиты коммерческой тайны	ОК-4, ОК-6, ОК-8	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Институт правовой защиты персональных данных	ОК-4, ОК-6, ОК-8	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Международное законодательство в области обеспечения информационной безопасности	ОК-4, ОК-6, ОК-8	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

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

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

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

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

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Остапенко, Г.А.Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия : Учеб. пособие / Г. А. Остапенко, Е. А. Мешкова ; под ред. В. Г. Кулакова. - М. : Горячая линия -Телеком, 2008. - 208 с. : ил . - ISBN 978-5-9912-0037-0 : 242-55.

8.2Переченьинформационныхтехнологий,используемыхприосуществленииобразовательногопроцессаподисциплине,включаяпереченьлице

нзионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

1. http://www.fsb.ru – сайт ФСБ РФ
2. http://www.fstec.ru – сервер ФСТЭК РФ
3. http://www.gov.ru – сервер органов государственной власти РФ
4. http://www.minsvyaz.ru – сайт министерства информационных технологий и связи РФ
5. http://www.scrf.gov.ru – сайт Совета Безопасности РФ
6. www.consultant.ru – Консультант плюс
7. https://gost.ru – Росстандарт
8. http://docs.cntd.ru – Электронный фонд правовой и нормативно-технической документации
9. http://www.securrity.ru – Сайт Информационная безопасность
10. https://www.securitylab.ru – Информационный портал по информационной безопасности
11. https://securelist.ru/ - Сетевая штаб-квартира экспертов «Лаборатории Касперского»
12. https://moodle.osu.ru - Электронные курсы ОГУ в системе обучения moodle
13. https://openedu.ru/course/hse/DATPRO/ - «Открытое образование». Курсы, МООК: Защита информации.
14. https://ru.coursera.org/learn/metody-i-sredstva-zashity-informacii - «Coursera». Курсы, МООК: Методы и средства защиты информации
15. https://ru.coursera.org/learn/management-informacionnoi-bezopasnosti - «Coursera». Курсы, МООК: Менеджмент информационной безопасности
16. https://www.intuit.ru/studies/courses/3648/890/info – «Интуит. Национальный открытый университет» Курсы, МООК: Аттестация объектов информатизации по требованиям безопасности информации.
17. https://www.intuit.ru/studies/courses/3601/843/info - «Интуит. Национальный открытый университет» Курсы, МООК: Информационное право: Информация.
18. https://openedu.ru/course/ITMOUniversity/INTPRO/- «Открытое образование» Курсы, МООК: Правовые основы защиты интеллектуальной собственности

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

Учебные аудитории для проведения занятий лекционного типа

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Правовыеосновыобеспечениякомпьютернойбезопасности»читаютсялекции,проводятсяпрактическиезанятия.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяна

иболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Практическиезанятиянаправленынаприобретениепрактическихнавыковрасчетарисков в автоматизированных системах.Занятияпроводятсяпутемрешенияконкретныхзадачваудитории.

Видучебныхзанятий	Деятельностьстудента
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.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
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 с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.