Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО
К УТВЕРЖДЕНИЮ
Декан, председатель совета
факультета КТВТиЭ
_____ **Ш. А. Юсуфов**
«18» 10 2018 г.

УТВЕРЖДАЮ
Проректор по учебной работе,
председатель методического
совета ДГТУ
_____ **Н. С. Суракатов**
«21» 10 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина С1.Б.32 Управление информационной безопасности

для специальности 10.05.03-«Информационная безопасность автоматизированных систем»

специализация «Безопасность открытых информационных систем»

факультет «Компьютерных технологий, вычислительной техники и энергетики»
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) Специалист по защите информации
бакалавр (специалист)

Форма обучения очная ; курс4: семестр 9 :

Всего трудоемкость в зачетных единицах (часах) 5 ЗЕТ (180 часа)

Лекции 34 (час); экзамен 9 семестр (1 зет=36 часов)

практические (семинарские) занятия - (час): зачет - (семестр)

лабораторные занятия 34 (час): самостоятельная работа 76 (час):

курсовой проект (работа, РГР)-(семестр).

Зав. кафедрой ИБ _____ Г.И. Качаева
подпись

Начальник УО _____ Э.В. Магомаева
подпись

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем».

Программа одобрена на заседании выпускающей кафедры ИБ от 15.10.2018г., протокол № 2

Зав. выпускающей кафедрой по данной специальности _____ **Г.И. Качаева**

ОДОБРЕНО
Методической комиссией по укрупненным группам специальностей и направлению подготовки
10.00.00- «Информационная безопасность»
Председатель МК
_____ Мелехин В.Б.
подпись ИОФ

«15» 10 2018г.

АВТОР ПРОГРАММЫ

Качаева Г.И., к.э.н., ст. преп. каф. ИБ
И.О.Ф. уч. степень, ученое звание, подпись

1. Цели и задачи дисциплины

1.1 **Цели дисциплины**

Цель дисциплины - овладение основными принципами управления уровнем информационной безопасности защищаемых ресурсов организации.

1.2 Задачи дисциплины

Задачи изучения дисциплины:

- Получение студентами знаний о структуре и принципах построения политики информационной безопасности организации.
- Получение студентами умений и навыков по построению моделей угроз и нарушителей и по оценке рисков информационной безопасности в организации.
- Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.

2. Место дисциплины в структуре ООП специалитета

Дисциплина «Управление информационной безопасности» относится к базовой части ФГОС ВО.

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Безопасность жизнедеятельности, Безопасность операционных систем, Безопасность сетей ЭВМ, Безопасность систем баз данных, Документоведение, Моделирование автоматизированных информационных систем, Организационное и правовое обеспечение информационной безопасности, Теория вероятностей и математическая статистика, Техническая защита информации..

Последующими дисциплинами являются: Преддипломная практика, Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующей компетенции:

- способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);
- способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);
- способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);
- способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);
- способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);
- способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);
- способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

В результате изучения дисциплины студент должен

Знать:

- сущность и понятие информации, информационной безопасности и характеристику ее составляющих; источники и классификацию угроз информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);
- основные методы управления информационной безопасностью; методы аттестации уровня защищенности автоматизированных систем; принципы формирования политики информационной безопасности в автоматизированных системах;

уметь:

- анализировать и оценивать угрозы информационной безопасности объекта; разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; оценивать информационные риски в автоматизированных системах;
- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
- разрабатывать частные политики информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем;
- разрабатывать предложения.

владеть:

- по совершенствованию системы управления информационной безопасностью автоматизированных систем;
- профессиональной терминологией в области информационной безопасности; навыками работы с нормативными правовыми актами;
- методами организации и управления деятельностью служб защиты информации на предприятии;
- методами управления информационной безопасностью автоматизированных систем; методами формирования требований по защите информации; методами оценки информационных рисков

6. Структура и содержание дисциплины «Управление информационной безопасности»

Общая трудоемкость дисциплины составляет 5 зачетных единиц – 180 часов, в том числе: лекционных -34 часа, лабораторных - 34 часа, СРС – 76 часов, форма отчетности экзамен в 9 семестре.

4.1.Содержание дисциплины

	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего* контроля успеваемости *(по срокам текущих аттестаций в семестре)*
				ЛК	ПЗ	ЛР	СР	
1.	**Лекция №1 Тема: «Основы построения систем обеспечения информационной безопасности на предприятии»** Деятельность по обеспечению информационной безопасности. Предметная направленность деятельности по обеспечению информационной безопасности. Цель деятельности по обеспечению информационной безопасности. Принципы и форма деятельности по обеспечению информационной безопасности. Методы деятельности по обеспечению информационной безопасности. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности.	5	1	2		2	4	Вх. Контр.
2.	**Лекция № 2 Тема: «Обеспечение информационной безопасности бизнеса»** Информационная сущность бизнеса. Роль руководства организации в обеспечении информационной безопасности. Определение информационной безопасности. Правовая среда бизнеса и ее свойства. Внутренняя нормативная база организации. Модель информационной безопасности бизнеса. Обобщенная модель распределения ресурсов организации в условиях рисков. Ущерб и негативные последствия. Риск-ориентированный подход к обеспечению информационной безопасности бизнеса. Общая модель обеспечения ИБ бизнеса.		2	2		2	4	
3.	**Лекция № 3 Тема: «Система управления информационной безопасностью бизнеса»** Модели непрерывного совершенствования и корпоративное управление. Модели непрерывного совершенствования и международные стандарты. Шаги реализации стандартной системы управления информационной безопасностью организации. Модели COSO, COBIT, ITIL. Контроль и аудит.		3	2		2	4	
4.	**Лекция № 4 Тема: «Анализ объекта защиты»**		4	2		2	4	

	Технология анализа объекта защиты. Типы информационных систем. Методы оценки ущерба от реализации угроз информационной безопасности. Комплекс стандартов в области информационной безопасности.							
5.	**Лекция № 5 Тема: «Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса»** Способы оценки информационной безопасности. Основные элементы процесса оценки информационной безопасности. Способы измерения атрибутов объекта оценки информационной безопасности. Применение типовых моделей оценки на основе оценки процессов и уровней зрелости процессов для оценки информационной безопасности. Модель оценки информационной безопасности на основе оценки процессов. Риск-ориентированная оценка информационной безопасности.	5	2		2	4	АКР №1
6.	**Лекция № 6 Тема: «Модель угроз и модель нарушителя»** Подходы к формированию модели нарушителя и модели угроз. Требования регуляторов к формированию модели нарушителя и модели угроз.	6	2		2	4	
7.	**Лекция № 7 Тема: «Социальные аспекты системы управления информационной безопасностью бизнеса»** Формализованное представление угроз ИБ от персонала. Общая характеристика угроз ИБ от персонала. Формализованное представление угроз ИБ от персонала. Противодействие угрозам ИБ от персонала. Социальные аспекты угроз ИБ от персонала. Личность злоумышленника.	7	2			4	
8.	**Лекция № 8 Тема: «Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации»** Рискообразующие факторы. Структура информационного риска. Понятие «Риск информационной безопасности». Методика анализа риска информационной безопасности. Обработка рисков информационной безопасности. Процесс «Управление рисками информационной безопасности». Место управления рисками информационной безопасности в структуре управления операционными рисками организации. Место управления рисками информационной безопасности в структуре управления информационной безопасностью организации.	8	2		2	4	

9.	**Лекция № 9 Тема: «Оценка рисков информационной безопасности»** Основные положения стандартов в области управления рисками информационной безопасности.		9	2		2	6	
10.	**Лекция № 10 Тема: «Планирование деятельности по обработке рисков обеспечения информационной безопасности организации»** Обработка рисков информационной безопасности. Цели управления и средства обработки рисков информационной безопасности. Модель обработки рисков информационной безопасности ISO/IEC 27001. Понятие «критерий принятия риска». Методы трансформации рисков информационной безопасности. Анализ эффективности результатов обработки рисков.		10	2		2	4	АКР №2
11.	**Лекция № 11 Тема: «Система управления информационной безопасностью»** Основные положения стандартов по проектированию, реализации и аудиту системы управления информационной безопасностью. Организация управления персоналом в контексте обеспечения информационной безопасности.		11	2		2	4	
12.	**Лекции № 12 Тема: «Политика информационной безопасности»** Основные положения стандартов в об-ласти регламентации обеспечения ин-формационной безопасности.		12	2		2	6	
13.	**Лекции № 13 Тема: «Управление инцидентами информационной безопасности»** Основные положения стандартов в области управления инцидентами информационной безопасности. Регламентация действий сотрудников при возникновении нештатных ситуаций.		13	2		2	4	
14.	**Лекция № 14 Тема: «Инфраструктура информационной безопасности»** Безопасность доступа сторонних организаций. Идентификация рисков, связанных с подключениями сторонних организаций. Условия безопасности в контрактах, заключѐнных со сторонними организациями. Классификация ресурсов и их контроль. Ответственность за ресурсы. Классификация информации. Безопасность персонала. Безопасность в должностных инструкциях и при выделении ресурсов. Обучение пользователей. Реагирование на события, таящие угрозу безопасности.	8	14	2		2	4	
15.	**Лекция № 15 Тема: «Аудит методов и средств обеспечения информационной безопасности организации»** Аудит информационной безопасности.		15	2		2	6	АКР №3

	Стандарты и практики аудита информационной безопасности. Международный стандарт ISO 19011. Методы организации, подготовки и проведения аудита информационной безопасности. Обработка результатов аудита. Место аудита информационной безопасности в структуре управления информационной безопасностью организации.							
16.	**Лекция № 16** **Тема: «Физическая безопасность и безопасность окружающей среды»** Защищѐнные области. Защита оборудования. Администрирование компьютерных систем и вычислительный сетей. Операционные процедуры и обязанности. Планирование систем и их приѐмка. Защита от вредоносного программного обеспечения. Обслуживание систем. Оперирование с носителями информации и их защита. Обмен данными и программами.		16	2		2	6	
17.	**Лекция № 17** **Тема: «Управление доступом к системам»** Производственные требования к управлению доступом к системам. Управление доступом пользователей. Обязанности пользователей. Слежение за доступом к системам и их использованием. Разработка и сопровождение информационных систем. Требования к безопасности систем. Безопасность в прикладных системах. Защита файлов прикладных систем. Безопасность в среде разработки и рабочей среде. Вопросы бесперебойной работы организации. Выполнение правовых требований. Проверка безопасности информационных систем.		17	2		2	4	
	Итого по дисциплине			**34**		**34**	**76**	**зачет**

4.2. Содержание лабораторных занятий

№ п/п	№ лекции израбочей программы	Наименование лабораторных заняти1	Рекомендуемая литература и методические разработки (№ источника из списка литературы)	Кол-во часов
1	Лк №1	Основы построения систем обеспечения информационной безопасности на предприятии	№№ 1-17	2
2	Лк №2	Обеспечение информационной безопасности бизнеса	№№ 1-17	2
3	Лк №3	Система управления информационной безопасностью бизнеса	№№ 1-17	2
4	Лк № 4	Анализ объекта защиты	№№ 1-17	2

5	Лк № 5	Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса	№№ 1-17	2
6	Лк №6	Модель угроз и модель нарушителя	№№ 1-17	2
7	Лк № 7	Социальные аспекты системы управления информационной безопасностью бизнеса	№№ 1-17	2
8	Лк №8	Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации	№№ 1-17	2
9	Лк №9	Оценка рисков информационной безопасности»	№№ 1-17	2
10	Лк №10	Планирование деятельности по обработке рисков обеспечения информационной безопасности организации	№№ 1-17	
11	Лк №11	Система управления информационной безопасностью	№№ 1-17	2
12	Лк №12	Политика информационной безопасности	№№ 1-17	2
13	Лк №13	Управление инцидентами информационной безопасности	№№ 1-17	2
14	Лк №14	Инфраструктура информационной безопасности	№№ 1-17	2
15	Лк №15	Аудит методов и средств обеспечения информационной безопасности организации	№№ 1-17	2
16	Лк №16	Физическая безопасность и безопасность окружающей среды	№№ 1-17	2
17	Лк №17	Управление доступом к системам	№№ 1-17	2
Итого по дисциплине				**34**

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов из содержания дисциплины	Рекомендуемая литература и источники информации	Формаконтроля СРС
1.	Основы построения систем обеспечения информационной безопасности на предприятии	4	№№ 1-17	Опрос, реферат, статья
2.	Обеспечение информационной безопасности бизнеса	4	№№ 1-17	Опрос, реферат, статья
3.	Система управления информационной безопасностью бизнеса	4	№№ 1-17	Опрос, реферат, статья
4.	Анализ объекта защиты	4	№№ 1-17	Опрос, реферат, статья
5.	Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса	4	№№ 1-17	Опрос, реферат, статья
6.	Модель угроз и модель нарушителя	4	№№ 1-17	Опрос, реферат, статья
7.	Социальные аспекты системы управления информационной безопасностью бизнеса	4	№№ 1-17	Опрос, реферат, статья
8.	Методы управления информационными	4	№№ 1-17	Опрос, реферат,

	рисками. Анализ влияния информационного риска на деятельность организации			статья
9.	Оценка рисков информационной безопасности»	6	№№ 1-17	Опрос, реферат, статья
10.	Планирование деятельности по обработке рисков обеспечения информационной безопасности организации	4	№№ 1-17	Опрос, реферат, статья
11.	Система управления информационной безопасностью	4	№№ 1-17	Опрос, реферат, статья
12.	Политика информационной безопасности	6	№№ 1-17	Опрос, реферат, статья
13.	Управление инцидентами информационной безопасности	4	№№ 1-17	Опрос, реферат, статья
14.	Инфраструктура информационной безопасности	4	№№ 1-17	Опрос, реферат, статья
15.	Аудит методов и средств обеспечения информационной безопасности организации	6	№№ 1-17	Опрос, реферат, статья
16.	Физическая безопасность и безопасность окружающей среды	6	№№ 1-17	Опрос, реферат, статья
17.	Управление доступом к системам	4	№№ 1-17	Опрос, реферат, статья
Итого		**76**		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий.

При проведении занятий по учебной дисциплине рекомендуется следовать и традиционным технологиям, в частности, в каждом разделе курса выделять наиболее важные моменты, акцентировать на них внимание обучаемых.

При чтении лекций по всем разделам программы иллюстрировать теоретический материал большим количеством примеров, что позволит сделать изложение наглядным и продемонстрировать обучаемым приемы программирования.

При изучении всех разделов программы добиться точного знания обучаемыми основных исходных понятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно– методическое обеспечение самостоятельной работы студентов

Вопросы входного контроля для проверки знаний студентов

1. Информация и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?

Аттестационная контрольная работа №1

1. Основы построения систем обеспечения информационной безопасности на предприятии.
2. Обеспечение информационной безопасности бизнеса.
3. Система управления информационной безопасностью бизнеса.
4. Анализ объекта защиты.
5. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса.

Аттестационная контрольная работа №2

1. Модель угроз и модель нарушителя.
2. Социальные аспекты системы управления информационной безопасностью бизнеса.
3. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации.
4. Оценка рисков информационной безопасности.
5. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации.

Аттестационная контрольная работа №3

1. Система управления информационной безопасностью
2. Политика информационной безопасности
3. Управление инцидентами информационной безопасности
4. Инфраструктура информационной безопасности
5. Аудит методов и средств обеспечения информационной безопасности организации

Перечень вопросов на экзамен

1. Основы построения систем обеспечения информационной безопасности на предприятии.
2. Обеспечение информационной безопасности бизнеса.
3. Система управления информационной безопасностью бизнеса.
4. Анализ объекта защиты.
5. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса.
6. Модель угроз и модель нарушителя.
7. Социальные аспекты системы управления информационной безопасностью бизнеса.
8. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации.
9. Оценка рисков информационной безопасности.
10. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации.
11. Система управления информационной безопасностью.
12. Политика информационной безопасности.
13. Управление инцидентами информационной безопасности.
14. Инфраструктура информационной безопасности.

15. Аудит методов и средств обеспечения информационной безопасности организации.
16. Физическая безопасность и безопасность окружающей среды.
17. Управление доступом к системам.

Вопросы проверки остаточных знаний

18. Система управления информационной безопасностью.
19. Политика информационной безопасности.
20. Управление инцидентами информационной безопасности.
21. Инфраструктура информационной безопасности.
22. Аудит методов и средств обеспечения информационной безопасности организации.
23. Физическая безопасность и безопасность окружающей среды.
24. Управление доступом к системам.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля) «Управление информационной безопасности»

7.1. Рекомендуемая литература и источники информации

Зав. библиотекой _____

№	Виды заня-тий (лк, пр, лб, срс)	Комплект необходимой учебной лит-ры по дисциплинам (наименование учебника, пособия)	Авторы	Издат-во и год издания	Кол-во пособий, учебников и прочей литер-ры	
					в библ	на каф
ОСНОВНАЯ ЛИТЕРАТУРА						
1.	Лк, лб, срс	Теория информации и кодирования	Санников В.Г.	Московский технический университет связи и информатики, 2015.— 95 с	http://www.iprbookshop.ru/61558	
2.	Лк, пр, срс	Информационная безопасность и защита информации	Шаньгин, В. Ф.	Электрон. текстовые дан. – Москва : ДМК Пресс, 2014. – 702 с	http://www.iprbookshop.ru/29257	
3.	Лк, пр, срс	Современные системы управления информационной безопасностью: учебное пособие	А. Ж. Абденов, Г. А. Дронова, В. А.	Новосибирск: Новосибирский государственный технический университет, 2017. — 48 с. — ISBN 978-5-7782-3236-5.	http://www.iprbookshop.ru/91427.html	
4.		Управление информационной безопасностью: учебное пособие	А. К. Шилов	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018. — 120 с. — ISBN 978-5-9275-2742-7.	http://www.iprbookshop.ru/87643.html	
5.		Криптография и безопасность в технологии. NET [Электронный ресурс]	Торстейнсон П., Г.А. Ганеш.	М.: "Лаборатория знаний" (ранее "БИНОМ.Лаборатория знаний"), 2015. — 480 с.	http://e.lanbook.com/books/element.php?pl1_id=70724	
6.		Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие	Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин [и др.].	Воронеж: ВГУИТ (Воронежский государственный университет инженерных технологий), 2013. — 192 с.	http://e.lanbook.com/books/element.php?pl1_id=72884	
7.		Криптографическая защита информации. Учебное пособие [Электронный ресурс]: учебное пособие	Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев.	Спб.: НИУ ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики), 2012. — 142 с.	http://e.lanbook.com/books/element.php?pl1_id=40849	
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА						

8.	Лк, лб, срс	Интеллектуальные системы защиты информации [Электронный ресурс]: учебное пособие	Васильев В.И.	М.: Машиностроение, 2013. — 172 с.	http://e.lanbook.com/books/element.php?pl1_id=5792
9.	Лк, лб, срс	Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие	В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин [и др.]	М.: ФЛИНТА, 2011. — 187 с.	http://e.lanbook.com/books/element.php?pl1_id=60717
ИНТЕРНЕТ РЕСУРСЫ					
10.	ЛК,СР, КР	http://kmb.ufoctf.ru/index.html			
11.	ЛК,СР, КР	https://habrahabr.ru/hub/crypto/			
12.	ЛК,СР, КР	http://training.hackerdom.ru/			
13.	ЛК,СР, КР	http://fstec.ru/			
14.	ЛК,СР, КР	www.securitycode.ru - Код безопасности			
15.	ЛК,СР, КР	ru.wikipedia.org - википедия.			
16.	ЛК,СР, КР	www.rsl.ru - российская научная библиотека.			
17.	ЛК,СР, КР	www.iso27000.ru - Искусство управления информационной безопасностью. (Руководящие документы Гостехкомиссии, ФСТЭК, ФСБ).			

7.2. Программное обеспечение

Интегрированные среды разработки программ Borland Developer Studio и Visual Studio .NET, базы данных, информационно – справочные и поисковые системы; вузовские электронно-библиотечные системы учебной литературы; база научно-технической информации ВИНИТИ РАН.

8. Материально-техническое обеспечение дисциплины

При проведения лекционных и практических (семинарских) занятий предусматривается использование систем мультимедиа, программного обеспечения и информационных справочных систем:

1. Microsoft Office (Word, Excel, PowerPoint, Access)
2. ЭБС http://library.mirea.ru/.
3. Инструкция о порядке допуска должностных лиц и граждан РФ к государственной тайне. Постановление Правительства РФ от 6 февраля 2010 г. № 63
4. Международный стандарт ИСО/МЭК 27001. Первое издание 2005-1015. Информационные технологии. Методы защиты. Системы менеджмента защиты информации.
5. ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.
6. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
7. «Концепция информационной безопасности ФНС России»: Пр. ФНС России от 13.01.2012. № ММВ-7-4/6.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем».

Рецензент от выпускающей кафедры по специальности 10.05.03- «Информационная безопасность автоматизированных систем _____ З.Р. Рогожников
подпись, ФИО