Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра информационных технологий и систем безопасности

Рабочая программа дисциплины

Информационная безопасность в Интернете

Основная профессиональная образовательная программа
высшего образования по направлению подготовки

38.03.05 Бизнес-информатика

Направленность (профиль):

Бизнес-информатика

Уровень:
Бакалавриат

Форма обучения
Очная, заочная

Согласовано
Руководитель ОПОП

_____ **Степанов С.Ю.**

Утверждаю
Председатель УМС _____ **И.И. Палкин**

Рекомендована решением
Учебно-методического совета
11 июня **2019 г., протокол №** 7

Рассмотрена и утверждена на заседании кафедры
7 мая **2019 г., протокол №** 5
Зав. кафедрой _____ / Завгородний В.Н.

Авторы-разработчики:
_____ / Богданов П.Ю.

Санкт-Петербург 2019

1. Цели освоения дисциплины

Целью изучения дисциплины «Информационная безопасность в Интернете» является формирование у будущих специалистов комплекса компетенций, которые позволят им в будущей деятельности применять основы знаний по методам защиты информации, комплексному проектированию и анализу защищенных интернет-проектов (ИП).

Основные задачи дисциплины:

- изучить основы устройства и принципов функционирования ИП;
- изучить методологии проектирования и построения защищенных ИП;
- изучить критерии и методы оценки защищенности ИП, средств и методов защиты от несанкционированного доступа (НСД) к информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность в интернете» для направления подготовки 38.03.05 «Бизнес – информатика» является дисциплиной по выбору вариативного блока.

Для освоения данной дисциплины необходимо обладать базовыми знаниями (общее среднее образование), а также освоить учебный материал предшествующих дисциплин: «Основы Бизнес-информатики», «Информатика и программирование», «Автоматизация деловых процессов» «Информационная безопасность», «Бизнес-аналитика». Дисциплина является завершающей. Знания, полученные в ходе изучения дисциплины, могут быть использованы для написания выпускной квалификационной работы.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Компетенция
ОПК-1	Обладать способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культу-

	ры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-9	Организовывать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

В результате освоения компетенций в рамках дисциплины обучающийся должен:

Знать:

- угрозы и методы нарушения безопасности ИП;
- методологические и технологические основы комплексного обеспечения безопасности ИП;
- формальные модели, лежащие в основе систем защиты ИП;
- стандарты по оценке защищенности ИП и их теоретические основы.

Уметь:

- проводить анализ ИП с точки зрения обеспечения компьютерной безопасности;
- реализовывать системы защиты информации в ИП в соответствии со стандартами по оценке защищенности ИП;
- разрабатывать модели и политику безопасности;
- применять стандарты по оценке защищенности ИП при анализе и проектировании систем защиты информации в ИП.

Владеть:

- навыками распознавания типичных атак на защищенные ИП;
- навыками анализа угроз информации;
- навыками применения архитектуры защищенных систем;
- навыками перспективных направлений развития теории компьютерной безопасности.

Основные признаки проявленности формируемых компетенций в результате освоения дисциплины сведены в таблицу.

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Этап (уровень) освоения компетенции	Основные признаки проявленности компетенции (дескрипторное описание уровня)				
	1.	2.	3.	4.	5.
минимальный	не владеет	слабо ориентируется в терминологии и содержании	Способен выделить основные идеи текста, работает с критической литературой	Владеет основными навыками работы с источниками и критической литературой	Способен дать собственную критическую оценку изучаемого материала
	не умеет	не выделяет основные идеи	Способен показать основную идею в развитии	Способен представить ключевую проблему в ее связи с другими процессами	Может соотнести основные идеи с современными проблемами
	не знает	допускает грубые ошибки	Знает основные рабочие категории, однако не ориентируется в их специфике	Понимает специфику основных рабочих категорий	Способен выделить характерный авторский подход
базовый	не владеет	плохо ориентируется в терминологии и содержании	Владеет приемами поиска и систематизации, но не способен свободно изложить материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций	Способен сравнивать концепции, аргументированно излагает материал
	не умеет	выделяет основные идеи, но не видит проблем	Выделяет конкретную проблему, однако излишне упрощает ее	Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой	Аргументированно проводит сравнение концепций по заданной проблематике
	не знает	допускает много ошибок	Может изложить основные рабочие категории	Знает основные отличия концепций в заданной проблемной области	Способен выделить специфику концепций в заданной проблемной области
продвинутый	не владеет	ориентируется в терминологии и содержании	В общих чертах понимает основную идею, однако плохо связывает ее с существующей проблематикой	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области
	не умеет	выделяет основные идеи, но не видит их в разви-	Может понять практическое назначение основной идеи, но затрудняется выявить ее осно-	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет вы-

		тии	вания	испытывает затруднения в описании сложных объектов анализа	делить практическое значение заданной области
	не знает	допускает ошибки при выделении рабочей области анализа	Способен изложить основное содержание современных научных идей в рабочей области анализа	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить	Может дать критический анализ современным проблемам в заданной области анализа

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

Объем дисциплины (модуля) по видам учебных занятий

в академических часах)

2017, 2018

Объём дисциплины	**Всего часов**		
	Очная форма обучения	**Очно-заочная форма обучения**	**Заочная форма обучения**
Общая трудоёмкость дисциплины	**108**	**-**	**108**
Контактная работа обучающихся с преподавателям (по видам аудиторных учебных занятий) – всего:	**48**	**-**	**6**
в том числе:		**-**	**-**
лекции	**16**	**-**	**2**
практические занятия	**32**	**-**	**4**
семинарские занятия	**-**	**-**	**-**
Самостоятельная работа (СРС) – всего:	**60**	**-**	**102**
в том числе:	**-**	**-**	**-**
курсовая работа	**-**	**-**	**-**
контрольная работа	**-**	**-**	**-**
Вид промежуточной аттестации (зачет/экзамен)	**экзамен**	**-**	**-**

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов. 2019 г.

Объем дисциплины (модуля) по видам учебных занятий

в академических часах)

2019

Объём дисциплины	**Всего часов**		
	Очная форма обучения	**Очно-заочная форма обучения**	**Заочная форма обучения**
Общая трудоёмкость дисциплины	**108**	**-**	**108**
Контактная работа обучающихся с преподавателям (по видам аудиторных учебных занятий) – всего:	**42**	**-**	**12**
в том числе:		**-**	**-**

лекции	**14**	**-**	**4**
Лабораторные работы	**28**	**-**	**8**
семинарские занятия	**-**	**-**	**-**
Самостоятельная работа (СРС) – всего:	**66**	**-**	**96**
в том числе:	**-**	**-**	**-**
курсовая работа	**-**	**-**	**-**
контрольная работа	**-**	**-**	**-**
Вид промежуточной аттестации (зачет/экзамен)	**Зачет 8 сем**	**-**	**Зачет 5**

4.1. Структура дисциплины

Очная форма
2017, 2018

№ п/п	Раздел и тема дисциплины	Семестр	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля успеваемости	Занятия в активной и интерактивной форме, час.	Формируемые компетенции
			Лекции	Практика	Самост. работа			
1	Стандарты, спецификации и функциональные требования безопасности	7	5,3	10,6	20	Ответ на экзамене	-	ОПК-1
2	Требования доверия безопасности	7	5,3	10,6	20	Ответ на экзамене	-	ПК-9
3	Спецификации Интернет-сообществ	7	5,3	10,6	20	Ответ на экзамене	-	ПК-9
	ИТОГО		**16**	**32**	**60**			

Очная форма
2019

№ п/п	Раздел и тема дисциплины	Семестр	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля успеваемости	Занятия в активной и интерактивной форме, час.	Формируемые компетенции
			Лекции	Практика	Самост. работа			
1	Стандарты, спецификации и функциональные требования безопасности	8	5	8	20	Ответ на экзамене	-	ОПК-1
2	Требования доверия безопасности	8	5	8	20	Ответ на экзамене	-	ПК-9
3	Спецификации Интернет-сообществ	8	4	12	26	Ответ на экзамене	-	ПК-9
	ИТОГО		**14**	**28**	**66**			

Заочная форма

2018

№ п/п	Раздел и тема дисциплины	курс	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля успеваемости	Занятия в активной и интерактивной форме, час.	Формируемые компетенции
			Лекции	Практика	Самост. работа			
1	Стандарты, спецификации и функциональные требования безопасности	5	0,6	1,3	34	Ответ на экзамене	-	ОПК-1
2	Требования доверия безопасности	5	0,6	1,3	34	Ответ на экзамене	-	ПК-9
3	Спецификации Интернет-сообществ	5	0,6	1,3	34	Ответ на экзамене	-	ПК-9
	ИТОГО		**2**	**4**	**102**			

Заочная форма

2019

№ п/п	Раздел и тема дисциплины	курс	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля успеваемости	Занятия в активной и интерактивной форме, час.	Формируемые компетенции
			Лекции	Практика	Самост. работа			
1	Стандарты, спецификации и функциональные требования безопасности	5	1	2	30	Ответ на экзамене	-	ОПК-1
2	Требования доверия безопасности	5	1	3	30	Ответ на экзамене	-	ПК-9
3	Спецификации Интернет-сообществ	5	2	3	36	Ответ на экзамене	-	ПК-9
	ИТОГО		**4**	**8**	**96**			

4.2. Содержание разделов дисциплины

4.2.1. Тема 1. Стандарты, спецификации и функциональные требования безопасности.

Стандарты и спецификации в области информационной безопасности. Принципы стандартизации. Спецификация. Доверенная система.Уровень гарантированности. Периметр безопасности. Безопасность повторного использования. Классификация по требованиям безопасности. Сервис

безопасности. Руководящие документы Гостехкомиссии России. Архитектура безопасности. Концепция единого входа в сеть. Функциональные требования «Общих критериев».

4.2.2. Тема 2. Требования доверия безопасности.

Требования доверия безопасности. Профиль защиты. Задание по безопасности. Процедуры безопасности. Оценка безопасности. Методология оценки безопасности. Среда безопасности. Требования и цели безопасности. Функциональный пакет. Краткая и функциональная спецификация. Проекты верхнего и нижнего уровня. Входная, выходная задача и задача оценки. Технический отчет оценки. Рейтинг уязвимостей. Стойкость функций безопасности. Потенциал нападения. Генерация данных аудита безопасности. Хранение событий аудита безопасности. Механизмы одноразовой аутентификации. Многоаспектность информационной безопасности. Управление информационными потоками. Иерархические атрибуты безопасности.

4.2.3. Тема 3. Спецификации Интернет-сообществ.

Внешний, внутренний и скрытый канал. Защита остаточной информации. Невозможность обхода защитных средств. Согласованность данных функций безопасности. Обнаружение повторного использования. Срок действия функций безопасности. Управление сеансами работы пользователей.Краткая спецификация объекта оценки функции безопасности. Оценочный уровень доверия. Формальная, полуформальная и неформальная спецификация. Уровень абстракции. Подсистема и модуль модели жизненного цикла. Безопасность ИТ разработки. Обязанности разработчика и оценщика. Анализ глубины функционального тестирования. Анализ стойкости функции безопасности. Анализ скрытых каналов. План поддержки доверия. Анализ влияния на безопасность. Оценочный уровень доверия. Модель ISO/ OSI и стек протоколов TCP/IP. Анализ угроз информационной безопасности.Проблемы

безопасности межсетевых экранов. Персональные и распределенные экраны. Схемы сетевой защиты на базе межсетевых экранов. Особенности функционирования МЭ на различных уровнях модели OSI.. Выполнение функций посредничества. Функции межсетевых экранов. Основные функции подсистемы защиты ОС. Угрозы безопасности ОС. Проблемы обеспечения безопасности операционных систем. Подходы к построению защищенной операционной системы. Архитектура и основные функции подсистемы защиты операционных систем. Полномочия разграничения доступа с контролем информационных потоков. Строгая аутентификация, основанная на симметричных и асимметричных алгоритмах. Аутентификация на основе одноразовых паролей. Методы аутентификации, использующие пароли и PIN-коды. Аутентификация на основе одноразовых паролей. Аутентификация, авторизация и администрирование действий пользователей. Отечественные стандарты безопасности информационных технологий. Стандарты информационной безопасности в Интернете. Стандарты для беспроводных сетей. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий». Базовая и специализированная политика безопасности. Структура политики безопасности организации. Основные понятия политики безопасности. Пути решения проблем защиты информации в сетях. Способы обеспечения информационной безопасности сетей. Угрозы и уязвимости беспроводных сетей. Угрозы и уязвимости проводных корпоративных сетей.

4.3. Семинарские, практические, лабораторные занятия, их содержание

№ п/п	№ раздела дисциплины	Тематика практических занятий	Форма проведения	Формируемые компетенции
1	1	Разработка слайдов на тему «Модель ISO/ OSI и стек протоколов TCP/IP»	Практическая работа	ОПК-1
2	1	Составление описания анализ угроз информационной безопасности в ИП.	Практическая работа	ОПК-1

3	2	Составление таблицы взаимосвязи оценочного уровня доверия.	Практическая работа	ПК-9
4	2	Составление многоуровневой таблицы глубины функционального тестирования.	Практическая работа	ПК-9
5	3	Составление схемы взаимосвязи атак и инструментов атак на защищенные компьютерные системы	Практическая работа	ПК-9
6	3	Построение схемы анализа стойкости функции безопасности.	Практическая работа	ПК-9
7	3	Описание основных схем сетевой защиты на базе межсетевых экранов.	Практическая работа	ПК-9

5. Учебно-методическое обеспечение самостоятельной работы студентов и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Во время самостоятельной работы студенты готовят эссе по темам дисциплины.

Эссе – краткое свободное прозаическое сочинение, рассуждение небольшого объёма. Эссе выражает индивидуальные впечатления и соображения автора по конкретному вопросу и заведомо не претендует на определённую или исчерпывающую трактовку темы. Эссе предполагает субъективное мнение о чем-либо. Эссе должно содержать чёткое изложение сути проставленной проблемы, включать самостоятельно проведенный анализ этой проблемы, выводы, обобщающие авторскую позицию по поставленной проблеме.

Контроль исполнения самостоятельных работ осуществляется преподавателем с участием студентов в форме дискуссии и обсуждения эссе.

Темы эссе:

1. Отечественные стандарты безопасности информационных технологий.
2. Стандарты информационной безопасности в Интернете.
3. Выполнение функций посредничества.
4. План поддержки доверия. Анализ влияния на безопасность.
5. Строгая аутентификация, основанная на симметричных и асимметричных

алгоритмах.

6. Аутентификация на основе одноразовых паролей.
7. Методы аутентификации, использующие пароли и PIN-коды.
8. Аутентификация, авторизация и администрирование действий пользователей. Анализ скрытых каналов.
9. Проблемы безопасности межсетевых экранов.
10. Персональные и распределенные экраны.
11. Базовая и специализированная политика безопасности.
12. Структура политики безопасности организации.
13. Основные понятия политики безопасности.
14. Пути решения проблем защиты информации в сетях.
15. Способы обеспечения информационной безопасности сетей.

5.3. Промежуточный контроль: экзамен в 7 семестре.

Перечень вопросов к экзамену:

1. Стандарты и спецификации в области информационной безопасности.
2. Принципы стандартизации. Спецификация.
3. Доверенная система.
4. Уровень гарантированности.
5. Периметр безопасности.
6. Безопасность повторного использования.
7. Классификация по требованиям безопасности.
8. Сервис безопасности.
9. Руководящие документы Гостехкомиссии России.
10. Архитектура безопасности.
11. Концепция единого входа в сеть.
12. Функциональные требования «Общих критериев».
13. Требования доверия безопасности.
14. Профиль защиты.
15. Задание по безопасности.

16. Процедуры безопасности.
17. Оценка безопасности.
18. Методология оценки безопасности.
19. Среда безопасности.
20. Требования и цели безопасности.
21. Функциональный пакет.
22. Краткая и функциональная спецификация.
23. Проекты верхнего и нижнего уровня.
24. Входная, выходная задача и задача оценки.
25. Технический отчет оценки.
26. Рейтинг уязвимостей.
27. Стойкость функций безопасности.
28. Потенциал нападения.
29. Генерация данных аудита безопасности.
30. Хранение событий аудита безопасности.
31. Механизмы одноразовой аутентификации.
32. Многоаспектность информационной безопасности.
33. Управление информационными потоками.
34. Иерархические атрибуты безопасности.
35. Внешний, внутренний и скрытый канал.
36. Защита остаточной информации.
37. Невозможность обхода защитных средств.
38. Согласованность данных функций безопасности.
39. Обнаружение повторного использования.
40. Срок действия функций безопасности.
41. Управление сеансами работы пользователей.
42. Краткая спецификация объекта оценки функции безопасности.
43. Оценочный уровень доверия.
44. Формальная, полуформальная и неформальная спецификация.
45. Уровень абстракции.

46. Подсистема и модуль модели жизненного цикла.
47. Безопасность ИТ разработки. Обязанности разработчика и оценщика.
48. Анализ глубины функционального тестирования.
49. Анализ стойкости функции безопасности.
50. Анализ скрытых каналов.
51. План поддержки доверия.
52. Анализ влияния на безопасность.
53. Оценочный уровень доверия.
54. Модель ISO/ OSI и стек протоколов TCP/IP.
55. Анализ угроз информационной безопасности.
56. Проблемы безопасности межсетевых экранов.
57. Персональные и распределенные экраны.
58. Схемы сетевой защиты на базе межсетевых экранов.
59. Особенности функционирования МЭ на различных уровнях модели OSI.
60. Выполнение функций посредничества.
61. Функции межсетевых экранов.
62. Основные функции подсистемы защиты ОС.
63. Угрозы безопасности ОС.
64. Проблемы обеспечения безопасности операционных систем.
65. Подходы к построению защищенной операционной системы.
66. Архитектура и основные функции подсистемы защиты операционных систем.
67. Полномочия разграничения доступа с контролем информационных потоков.
68. Строгая аутентификация, основанная на симметричных и асимметричных алгоритмах.
69. Аутентификация на основе одноразовых паролей.
70. Методы аутентификации, использующие пароли и PIN-коды.
71. Аутентификация на основе одноразовых паролей.
72. Аутентификация, авторизация и администрирование действий пользователей.

73. Отечественные стандарты безопасности информационных технологий.
74. Стандарты информационной безопасности в Интернете.
75. Стандарты для беспроводных сетей.
76. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий».
77. Базовая и специализированная политика безопасности.
78. Структура политики безопасности организации.
79. Основные понятия политики безопасности.
80. Пути решения проблем защиты информации в сетях.
81. Способы обеспечения информационной безопасности сетей.
82. Угрозы и уязвимости беспроводных сетей.
83. Угрозы и уязвимости проводных корпоративных сетей.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. Режим доступа: https://biblio-online.ru/book/44CE6B76-7554-4E65-BC10-D7F267D88DD0/informacionnaya-bezopasnost
2. Касьянов, В. В. Социология интернета : учебник для академического бакалавриата / В. В. Касьянов, В. Н. Нечипуренко. — М. : Издательство Юрайт, 2018. — 424 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-04944-2. — Режим доступа : www.biblio-online.ru/book/BDF8A753-0CE5-42C4-B936-6B017972744E.

б) дополнительная литература:

1. Полякова Т.А. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; отв. ред. Т. А. Полякова, А. А. Стрельцов. — М. : Издательство Юрайт, 2017. — 325 с

режим доступа: https://biblio-online.ru/book/EF942E2F-1F06-44B2-B4E3-65F9A13F2735/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti.

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2018. — 312 с. — (Серия : Специалист). — ISBN 978-5-9916-9043-0. — Режим доступа : www.biblio-online.ru/book/E458AFCD-826E-4A1F-9BAB-68BB83EA616F.
3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. — М. : Издательство Юрайт, 2018. — 349 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — Режим доступа : www.biblio-online.ru/book/59BABD78-5536-4ED4-BB9D-55E2F19F80B2.

Нормативная литература:

1. Закон РФ «О техническом регулировании» от 27 декабря 2002 г. №184-ФЗ (в ред. Федеральных законов от 09.05.2005 N 45-ФЗ, от 01.05.2007 N 65-ФЗ, от 01.12.2007 N 309-ФЗ, от 23.07.2008 N 160-ФЗ, действующая редакция от 29.06.2015)

2. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 31.12.2014) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.09.2015)

3. Федеральный закон от от 04.05.2011 N 99-ФЗ «О лицензировании отдельных видов деятельности» (действующая редакция от 13.07.2015)

4. Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации 09 сентября 2000 г. № Пр-1895)

5. Концепция развития национальной системы стандартизации Москва, 2 марта 2006 г., N 0392

6. Государственный стандарт российской федерации ГОСТ Р ИСО/МЭК 12207-99 - Процессы жизненного цикла программного обеспечения.

7. Государственный стандарт российской федерации ГОСТ Р ИСО/МЭК 15504

ТО (ISO/IEC TR 15504-CMM) - Оценка и аттестация зрелости процессов создания и сопровождения программных средств и информационных систем.
8. Государственный стандарт российской федерации ГОСТ Р ИСО/МЭК 14764 (сопровождение ПС).
9. Государственный стандарт российской федерации ГОСТ Р ИСО/МЭК 15026 (оценка уровня целостности систем и ПС).
10. Государственный стандарт российской федерации ГОСТ Р ИСО/МЭК 15910 (процессы создания документации пользователя ПС).
11. Государственный стандарт российской федерации ГОСТ Р ИСО/МЭК 15408 (ч. 1-3) (общие критерии оценки безопасности информационных технологий)
12. ГОСТ Российской Федерации - 1.0-2004 "Стандартизация в Российской Федерации. Основные положения".
13. ИСО/МЭК ТО 13335-3:1998 "Информационная технология. Рекомендации по менеджменту безопасности информационных технологий. Часть 3. Методы менеджмента безопасности информационных технологий".
14. ИСО/МЭК 13335-4:2004 Информационная технология. Рекомендации по менеджменту безопасности информационных технологий. Часть 4. Выбор мер защиты.
15. Федеральный закон от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании"

в) программное обеспечение и Интернет-ресурсы:

Программно-информационное обеспечение учебного процесса включает:

- Операционная система: Windows 7.
- Офисный пакет: Microsoft Office 2007.
- Электронная библиотека ЭБС «Znanium» [Электронный ресурс]. Режим доступа: http://znanium.com/
- Электронная библиотека ЭБС «Юрайт» [Электронный ресурс]. Режим доступа: https://biblio-online.ru/

– *Сайт Института развития информационного общества* [Электронный ресурс]. Режим доступа: http://www.iis.ru
– Сайт научно-аналитического журнала «Информационное общество» [Электронный ресурс]. Режим доступа: http://www.infosoc.iis.ru
– *Энциклопедия информационного общества* [Электронный ресурс]. Режим доступа: http://wiki.iis.ru

7. Методические указания для обучающихся по освоению дисциплины

вид учебных занятий	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практикум	Методические указания по выполнению лабораторных работ находятся на кафедре Прикладной информатики.
Самостоятельная работа	Работа с литературой, Интернет-ресурсами; выполнение заданий
Подготовка к экзамену	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Тема (раздел) дисциплины	Образовательные и информационные технологии	Перечень программного обеспечения и информационных справочных систем
Темы №1 – №3	Проведение лекций с использованием слайд-презентаций.	Операционная система: Windows 7. Офисный пакет: Microsoft Office 2007.

9. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы

с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

10. Материально-техническое обеспечение дисциплины

Материально-техническое обеспечение дисциплины соответствует действующим санитарно-техническим и противопожарным правилам и нормам и обеспечивает проведение всех видов лекционных, практических, лабораторных занятий и самостоятельной работы бакалавров.

Учебный процесс обеспечен аудиториями, комплектом лицензионного программного обеспечения, библиотекой РГГМУ.

Учебная аудитории для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).

Учебная аудитории для проведения занятий практического типа - укомплектована специализированной (учебной) мебелью, презентационной переносной техникой (проектор, ноутбук).

Учебная аудитория для курсового проектирования (выполнения курсовых работ) - укомплектована специализированной (учебной) мебелью.

Учебная аудитория для групповых и индивидуальных консультаций - укомплектована специализированной (учебной) мебелью, презентационной пе-

реносной техникой (проектор, ноутбук).

Учебная аудитория для текущего контроля и промежуточной аттестации - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации

Лаборатория (компьютерный класс) – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет", обеспечено доступом в электронную информационно-образовательную среду организации, установлено необходимое специализированное программное обеспечение.