Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Сибирский институт управления – филиал РАНХиГС
Факультет государственное и муниципальное управление

Кафедра информатики и математики

УТВЕРЖДЕНА
кафедрой информатики и математики
Протокол от «28» июня 2019 г. №10

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

Информационная безопасность

Б1.В.ДВ.03.01

не устанавливается

по направлению подготовки 38.03.04 Государственное и муниципальное управление направленность (профиль): «Информационные технологии в ГМУ» квалификация выпускника: бакалавр

формы обучения: очная

Год набора – 2021

Новосибирск, 2020

Автор–составитель:

Канд.техн.наук,, доцент кафедры информатики и математики

Терещенко Сергей Николаевич

Заведующий кафедрой информатики и математики

Рапоцевич Е. А.

СОДЕРЖАНИЕ

1 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина Б1.В.ДВ.03.01 «Информационная безопасность» обеспечивает овладение следующими компетенциями:

Таблица 1.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-6	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Очная форма обучения – ОПК-6.3	способность применять информационно-коммуникационные технологий с учетом основных требований информационной безопасности

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Таблица 2.

Профессиональные действия	Код этапа освоения компетенции	Результаты обучения
	Очная форма обучения – ОПК-6.3	на уровне знаний: основ информационной безопасности. на уровне умений: анализировать риски информационной безопасности на уровне навыков: навыками анализа угроз информационной безопасности

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Дисциплина Б1.В.ДВ.03.01 «Информационная безопасность» изучается на 4 курсе (8 семестр) очной формы обучения.

Количество академических часов, выделенных на контактную работу с преподавателем.

очная форма обучения

- 44 часов (12 часа лекций, 32 часа практических (семинарских) занятий);

на самостоятельную работу обучающихся – 64 часов.

Форма промежуточной аттестации в соответствии с учебным планом – зачет.

Место дисциплины

Освоение дисциплины опирается на минимально необходимый объем теоретических знаний в области информационных технологий, а также на приобретенные ранее умения и навыки использования информационных технологий в профессиональной деятельности.

Дисциплина реализуется после изучения: Б1.Б.09 Информационные технологии в управлении.

3. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Таблица 3.

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущ. контроля успеваемости[1], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			л	лр	пз	**КСР**		
Очная форма обучения								
Раздел 1	**Основы информационной безопасности**	***56***	***4***		***18***		***34***	
Тема1.1.	Введение в информационную безопасность системы управления				2		6	О - 1.1.
Тема 1.2.	Анализ рисков и оборонительные модели организации		1		4		8	О – 1.2 ПЗ – 1.2
Тема 1.3.	Политика безопасности		1		4		6	О - 1.3. ПЗ – 1.3
Тема 1.4.	Аутентификация и авторизация		1		4		6	О - 1.4. ПЗ – 1.4
Тема 1.5.	Архитектура безопасности		1		4		8	О - 1.5. ПЗ – 1.5
Раздел 2	**Разработка системы информационной безопасности**	***52***	***8***		***14***		***30***	
Тема 2.1	Межсетевые экраны		1		2		6	О – 2.1, ПЗ – 2.1
Тема 2.2.	Системы обнаружения атак		2		2		6	О – 2.2, ПЗ – 2.2
Тема 2.3.	Атака и методы хакеров		2		4		6	О – 2.3, ПЗ – 2.3

1 Формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), практические задания (ПЗ)

Тема 2.4.	Частные виртуальные сети		1		2		6	О – 2.4, ПЗ – 2.4
Тема 2.5.	Безопасность беспроводных сетей		2		4		6	О – 2.5,
Промежуточная аттестация								Зачет
Всего:		108	12		32		64	

Содержание дисциплины

Раздел 1. Основы информационной безопасности

Тема 1.1. Введение в информационную безопасность

Понятие информационной безопасности. Роль информационной безопасности в современном мире. Роль информационной безопасности в органах ГМУ. История безопасности. Компоненты защиты. Комплексный подход к обеспечению информационной безопасности. Лицензирование деятельности в области защиты информации. Сертификация средств защиты информации. Законодательство в сфере информационной безопасности в органах ГМУ.

Тема 1.2. Анализ рисков и оборонительные модели

Понятие рисков. Информационные риски в органах ГМУ. Векторы угроз. Модели защиты. Периметровая защита. Многоуровневая защита. Зоны доверия. Сегментация.

Тема 1.3. Политика безопасности

Понятие политики безопасности. Назначение политики безопасности. Разработка политики безопасности. Примеры политик безопасности. Политика безопасности в органах ГМУ.

Тема 1.4. Аутентификация и авторизация

Понятие аутентификации. Средства контроля аутентификации. Аутентификация по сертификатам. Защита ключей в системах аутентификации. Авторизация.

Тема 1.5. Архитектура безопасности

Конфиденциальность информации. История шифрования. Алгоритмы шифрования. Целостность информации. Доступность информации. Вирусы. Антивирусы. Стратегия песочницы.

Раздел 2. Разработка системы информационной безопасности

Тема 2.1. Межсетевые экраны

Понятие межсетевого экрана. Классификация МЭ. Шлюзы приложений и контурного уровня. Межсетевые экраны с адаптивной проверкой пакетов.

Тема 2.2. Системы обнаружения атак

Понятие системы обнаружения атак. Виды систем обнаружения атак. Модель обнаружения аномалий. Журналы и оповещения.

Тема 2.3. Атака и методы хакеров

Технология атаки. Атаки доступа. Атаки модификации. Маскарад. Переполнение буфера. Методы хакеров. Отказ в обслуживании. Распределенные атаки. Выполнение атак.

Тема 2.4. Частные виртуальные сети

Понятие частной виртуальной сети. VPN туннели. Протокол IPSec. Средства VPN. Установка VPN туннеля. VPN в органах ГМУ.

Тема 2.5. Безопасность беспроводных сетей

Беспроводные сети. Средства безопасности беспроводных сетей. Протокол WEP. Протокол WPA. Фильтрация MAC-адресов.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 4.

Тема (раздел)		Методы текущего контроля успеваемости
Раздел 1	**Основы информационной безопасности**	
Тема1.1.	Введение в информационную безопасность системы управления	Устный ответ на вопросы
Тема 1.2.	Анализ рисков и оборонительные модели организации	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 1.3.	Политика безопасности	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 1.4.	Аутентификация и авторизация	Устный ответ на вопросы
Тема 1.5.	Архитектура безопасности	Устный ответ на вопросы Выполнение практического задания на компьютере
Раздел 2	**Разработка информационно-аналитических систем**	
Тема 2.1	Межсетевые экраны	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 2.2.	Системы обнаружения атак	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 2.3.	Атака и методы хакеров	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 2.4.	Частные виртуальные сети	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 2.5.	Безопасность беспроводных сетей	Устный ответ на вопросы

4.1.2. Зачет проводится в форме устного ответа на вопрос.

4.2. Материалы текущего контроля успеваемости.

ТИПОВЫЕ ВОПРОСЫ И ЗАДАНИЯ ДЛЯ УСТНОГО (ПИСЬМЕННОГО) ОПРОСА

Тема 1.1. Введение в информационную безопасность системы управления (О - 1.1)

1. Компоненты защиты информационной безопасности.
2. Комплексный подход к обеспечению информационной безопасности.
3. Сертификация средств защиты информации.

Тема 1.2. Анализ рисков и оборонительные модели организации (О - 1.2)

1. Понятие рисков.
2. Что такое векторы угроз?
3. Какие существуют модели защиты?
4. Периметровая защита.

Тема 1.3. Политика безопасности (О - 1.3)

1. Для чего нужна политика безопасности?
2. Какие подразделения участвуют в разработке политики безопасности?
3. Каково содержание политики безопасности?

Тема 1.4. Аутентификация и авторизация (О - 1.4)

1. Понятие аутентификации.
2. Средства контроля аутентификации.
3. Аутентификация по сертификатам.
4. Защита ключей в системах аутентификации.

Тема 1.5 Аутентификация и авторизация (О - 1.5)

1. Целостность информации.
2. Доступность информации.
3. Вирусы и антивирусы.

Тема 2.1. Межсетевые экраны (О - 2.1)

1. Классификация МЭ.
2. Шлюзы приложений и контурного уровня.

Тема 2.2. Системы обнаружения атак (О - 2.2)

1. Понятие системы обнаружения атак.
2. Виды систем обнаружения атак.
3. Модель обнаружения аномалий

Тема 2.3. Атака и методы хакеров (О - 2.3)

1. Атаки доступа.
2. Атаки модификации.
3. Переполнение буфера.

4. Распределенные атаки.

Тема 2.4. Частные виртуальные сети (О - 2.4)

1. Понятие частной виртуальной сети.
2. VPN туннели.
3. Протокол IPSec.

Тема 2.5. Безопасность беспроводных сетей (О - 2.5)

1. Средства безопасности беспроводных сетей.
2. Протокол WEP.
3. Протокол WPA.

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Тема 1.2. Анализ рисков и оборонительные модели организации (ПЗ – 1.2)

1. Создайте модель угроз для университета.
2. Создайте модель угроз для банка.

Тема 1.3. Политика безопасности (ПЗ – 1.3)

1. Создайте политику безопасности для университета.
2. Создайте политику безопасности для банка.

Тема 1.5. Архитектура безопасности (ПЗ – 1.5)

1. Создайте архитектуру безопасности для университета.
2. Создайте архитектуру безопасности для банка.

Тема 2.1. Межсетевые экраны (ПЗ – 2.1)

1. Создайте модель межсетевых экранов для сети университета.
2. Создайте модель межсетевых экранов для сети банка.

Тема 2.2. Системы обнаружения атак (ПЗ – 2.2)

1. Создайте модель системы обнаружения атак для сети университета.
2. Создайте модель системы обнаружения атак для сети банка.

Тема 2.3. Атака и методы хакеров (ПЗ – 2.3)

1. Создайте программное обеспечение на C#, имитирующее атаку доступа.
2. Создайте программное обеспечение на C#, имитирующее SQL-инъекцию.

Тема 2.4. Частные виртуальные сети (ПЗ – 2.4)

1. Создайте частную виртуальную сеть.

Тема 2.5. Безопасность беспроводных сетей (ПЗ – 2.5)

1. Создайте частную виртуальную сеть.

4.3. Оценочные средства промежуточной аттестации

Таблица 5.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-6	способность решать стандартные задачи профессиональной деятельности на основе информационной и	Очная форма обучения – ОПК-6.3	способность применять информационно-коммуникационные технологий с учетом основных требований информационной безопасности

	библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		

Таблица 6.

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ОПК-6.3 способность применять информационно-коммуникационные технологий с учетом основных требований информационной безопасности	Знает нарушения информационной безопасности компьютерной системы и их причины Умеет проводить сертификацию средств защиты информации	Осуществляет политику безопасности компьютерной системы Проводит политику безопасности беспроводных сетей

ТИПОВЫЕ ВОПРОСЫ И ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
2. Законодательство в сфере информационной безопасности.
3. Лицензирование деятельности в области защиты информации.
4. Нарушения информационной безопасности компьютерной системы и их причины.
5. История компьютерной безопасности.
6. Понятие угрозы.
7. Сертификация средств защиты информации.
8. Политика безопасности.
9. Организационные меры по защите информации.
10. Принципы криптографической защиты информации.
11. Информационная безопасность в органах ГМУ.
12. Алгоритм блочного шифрования DES.
13. Алгоритм шифрования с открытым ключом RSA.
14. Блочные и поточные алгоритмы шифрования.
15. Алгоритм электронной цифровой подписи RSA.
16. Типовые схемы идентификации и аутентификации пользователя.
17. Биометрическая идентификация и аутентификация пользователя.
18. Протокол SSL.
19. Центры сертификации.
20. Понятие о типах вирусов и способы защиты.
21. Защита от троянских программ.

22. Защита электронной почты.
23. Защита локальной рабочей станции.
24. Защита локальной сети.
25. Межсетевые экраны и особенности их функционирования.
26. Основные компоненты межсетевых экранов.
27. Системы обнаружения вторжений.
28. Управление журналами и оповещениями.
29. Методы хакеров.
30. Атаки на отказ в обслуживании.
31. Распределенные атаки.
32. Переполнение буфера.
33. Снифферы и спуфферы.
34. SQL-инъекции.
35. Социальный инжиниринг.
36. VPN.
37. Протокол IPsec.
38. Средства VPN.
39. Безопасность беспроводных сетей.
40. Технологии взлома беспроводных сетей.

.

4.4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Зачет включает ответы на устные теоретические вопросы.

Ответы на теоретические вопросы могу даваться в устной форме или в форме электронного тестирования.

Для получения положительной оценки на зачете достаточно изучить рекомендуемую основную литературу, а также усвоить умения и навыки в ходе контактной работы с преподавателем путем опроса и выполнения различных практических заданий.

Студент при подготовке к ответу по билету формулирует ответ на вопрос.

При подготовке ответа на вопрос стоит использовать соответствующий дисциплине понятийный аппарат.

Давать односложные ответы нежелательно.

ТИПОВЫЕ БИЛЕТЫ К ЗАЧЕТУ

Билет 1.
Вопрос: Политика безопасности.

Билет 2.
Вопрос: SQL-инъекции.

Ответ на вопрос билета оценивается по системе зачет/не зачет.

Шкала оценивания

Таблица 7

Зачет	Критерии оценки

не зачтено	Этапы компетенций, предусмотренные образовательной программой не сформированы. Недостаточный уровень усвоения понятийного аппарата и наличие фрагментарных знаний по дисциплине. Отсутствие минимально допустимого уровня в самостоятельном решении практических задач. Практические навыки профессиональной деятельности не сформированы.
зачтено	Этапы компетенций, предусмотренные образовательной программой сформированы. Наличие допустимого уровня в усвоении учебного материала, в т.ч. в самостоятельном решении практических задач. Практические навыки профессиональной деятельности сформированы.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При изучении курса «Информационная безопасность» применяются разнообразные лекции, практические занятия, выполнение практических заданий по темам, самостоятельная работа с источниками и др.).

Студент должен посетить установочные лекции, на которых излагается цель, задачи и содержание курса, приводятся рекомендации и критерии оценивания.

В ходе лекционных занятий раскрываются базовые вопросы в рамках каждого модуля дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала, даются рекомендации по выполнению заданий к практическим занятиям.

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям, а также к промежуточной аттестации по дисциплине.

Практические занятия позволяют более детально проработать наиболее важные темы курса. Целью практических занятий является закрепление теоретических знаний, полученных студентами на лекциях и в процессе самостоятельной работы, контроль за степенью усвоения пройденного материала, ходом выполнения студентами самостоятельной работы и рассмотрение наиболее сложных и спорных вопросов в рамках темы занятия.

Подготовку к занятиям следует начинать с ознакомления с содержанием темы, вопросами к теме, подбора рекомендованной литературы. Затем необходимо перечитать запись лекции, соответствующие разделы учебника, статьи в журналах. При этом перед собой нужно иметь соответствующие нормативные акты в действующей редакции.

Подготовка к практическим занятиям осуществляется студентами самостоятельно с использованием научной и учебной литературы и необходимых правовых источников. На практических занятиях у студентов формируются навыки публичного выступления, анализа материала, умение грамотно и обоснованно отвечать на поставленные вопросы и применять полученные теоретические знания к практическим ситуациям, а также умение решать практические задания (задачи).

Для получения глубоких теоретических знаний и практических навыков студентам рекомендуется посещать лекции, активно участвовать в практических занятиях. Поставленные перед занятиями цели могут быть достигнуты лишь при систематической работе студентов над изучением дисциплины.

При необходимости в период самостоятельной подготовки студенты могут получить индивидуальные консультации преподавателя по учебной дисциплине.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ПОДГОТОВКИ К ОПРОСУ

Опрос в рамках изучаемой темы может проходить как в устной, так и в письменной форме.

Опрос проводится только после изучения материала темы и направлен на ее закрепление.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ РЕШЕНИЯ ПРАКТИЧЕСКИХ ЗАДАНИЙ

Решение практических заданий нацелено на формирование у студента соответствующих компетентностных практических умений и владений. Поэтому для исключения компиляций результата все задания выполняются на компьютерах.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература.

1. Артемов, А. В. Информационная безопасность [Электронный ресурс] : учеб. пособие / А. В. Артемов. — Электрон. дан. – Орел : МАБИВ, 2014. — 256 с. — Доступ из ЭБС «IPRbooks». - Режим доступа : http://www.iprbookshop.ru/33430, требуется авторизация (дата обращения : 02.11.2016). – Загл. с экрана. - То же [Электронный ресурс]. - Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=428605, требуется авторизация (дата обращения : 19.12.2016). — Загл. с экрана.

2. Информационная безопасность России : учеб. пособие / А. П. Барановский [и др.] ; М-во образования и науки РФ, Сиб. гос. технол. ун-т [и др.]. - Красноярск : СибГТУ, 2011. - 123 с.

3. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Электрон. дан. – Москва : Евразийский открытый ин-т, 2012. - 311 с. - Доступ из ЭБС «IPRbooks». - Режим доступа : http://www.iprbookshop.ru/10677, требуется авторизация (дата обращения : 09.11.2016). - Загл. с экрана.

4. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / С. А. Нестеров ; Санкт-Петербургский государственный политехнический университет. - Электрон. дан. – Санкт-Петербург : Издательство Политехнического университета, 2014. - 322 с. - Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=363040, требуется авторизация (дата обращения : 19.12.2016). — Загл. с экрана. - То же [Электронный ресурс]. — Доступ из ЭБС «IPRbooks». — Режим доступа : http://www.iprbookshop.ru/43960, требуется авторизация (дата обращения : 19.12.2016). — Загл. с экрана.

5. Технологии защиты информации в компьютерных сетях [Электронный ресурс] / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. - 2-е изд., испр. - Электрон. дан. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. – Доступ из Унив. б-ки ONLINE. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=428820, требуется авторизация (дата обращения : 09.11.2016). — Загл. с экрана.

6.2. Дополнительная литература

1. Басалова, Г. В. Основы криптографии [Электронный ресурс] / Г. В. Басалова. — Электрон. дан. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 282 с. — Доступ из ЭБС «IPRbooks». — Режим доступа : http://www.iprbookshop.ru/52158, требуется авторизация (дата обращения : 19.12.2016). — Загл. с экрана.

2. Башлы, П. Н. Информационная безопасность : учеб-практическое пособие [Электронный ресурс] / П. Н. Башлы, Е. К. Баранова, А. В. Бабаш. - Электрон. дан. –

Москва : Евразийский открытый институт, 2011. - 375 с. - Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=90539, требуется авторизация (дата обращения : 19.12.2016). — Загл. с экрана.

3. Безопасность систем баз данных [Электронный ресурс] : учеб. пособие / А. В. Скрыпников [и др.]. — Электрон. дан. — Воронеж : Воронежский государственный университет инженерных технологий, 2015. — 144 с. — Доступ из ЭБС «IPRbooks». - Режим доступа : http://www.iprbookshop.ru/50628, требуется авторизация (дата обращения : 19.11.2016). — Загл. с экрана.

4. Галатенко, В. А. Основы информационной безопасности [Электронный ресурс] / В. А. Галатенко. – Электрон. дан. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — Доступ из ЭБС «IPRbooks». - Режим доступа : http://www.iprbookshop.ru/52209, требуется авторизация (дата обращения : 09.11.2016). – Загл. с экрана

5. Загинайлов, Ю. Н. Основы информационной безопасности [Электронный ресурс] : курс визуальных лекций : учебное пособие / Ю. Н. Загинайлов. - Электрон. дан. – Москва ; Берлин : Директ-Медиа, 2015. - 105 с. - Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=362895, требуется авторизация (дата обращения : 19.12.2016). — Загл. с экрана.

6. Кияев, В. Безопасность информационных систем [Электронный ресурс] : курс / В. Кияев, О. Граничин. - Электрон. дан. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. - Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=429032, требуется авторизация (дата обращения : 19.12.2016). — Загл. с экрана.

7. Организация безопасной работы информационных систем [Электронный ресурс] : учеб. пособие / Ю. Ю. Громов, Ю. Ф. Мартемьянов, Ю. К. Букурако и др. ; Тамбовский государственный технический университет. - Электрон. дан. – Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с. - Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=277794, требуется авторизация (дата обращения : 19.12.2016). — Загл. с экрана.

8. Петров, С. В. Информационная безопасность [Электронный ресурс] : учеб. пособие / С. В. Петров, П. А. Кисляков. — Электрон. дан. — Саратов : Ай Пи Ар Букс, 2015. — 326 с. — Доступ из ЭБС «IPRbooks». — Режим доступа : http://www.iprbookshop.ru/33857, требуется авторизация (дата обращения : 19.12.2016). — Загл. с экрана.

9. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Доступ из ЭБС «IPRbooks». — Режим доступа : http://www.iprbookshop.ru/29257, требуется авторизация (дата обращения : 19.12.2016). — Загл. с экрана.

6.3. Интернет-ресурсы

1. Бизнес и компьютер [Электронный ресурс]: офиц. сайт. – Режим доступа: http://www.bizcom.ru

2. Университетская библиотека ONLINE [Электронный ресурс]: [электрон.-библиотеч. система] / О-во с огранич. ответственностью «Директ-Медиа». - [М.], 2001 - 2010. - Режим доступа: http://www.biblioclub.ru, требуется авторизация.
3. Университетская информационная система РОССИЯ [Электронный ресурс] : тематич. электрон. б-ка / Науч.-исслед. вычислит. центр МГУ; Автоном. некоммерч. организация «Центр информац. исслед.». – Электрон. дан. – М., 2000 – 2012. - Режим доступа: http://uisrussia.msu.ru, требуется авторизация.

7. Материально – техническая база, информационные технологии, программное обеспечение и информационные справочные системы

7.1. Программное обеспечение

1. Microsoft Visual Studio 2010 и выше.
2. Microsoft SQL Server 2008 и выше.

7.2. Технические средства и материально-техническое обеспечение дисциплины (модуля).

Наименование специальных помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**
Учебные аудитории для проведения занятий лекционного типа (ауд. № 219)	экран, компьютер с подключением к локальной сети института, и выходом в Интернет, мультимедийный проектор, столы аудиторные, стулья, трибуна настольная, доска аудиторная
Лаборатория личностного и профессионального развития (ауд. № 219)	экран, компьютер с подключением к локальной сети института, и выходом в Интернет, мультимедийный проектор, столы аудиторные, стулья, трибуна настольная, доска аудиторная
Аудитория для самостоятельной работы обучающихся. Центр Интернет-ресурсов (ауд.№ 207, №208)	Мультимедийный проектор – 1шт., Экран проекционный – 1шт., Принтер-1шт. ПК - 11 шт. с подключенным интернетом и к локальной сети института (включая правовые системы) и Интернет, столы аудиторные, стулья, доски аудиторные.
Центр интернет-ресурсов (ауд. № 201)	10 компьютеров с выходом в Интернет, автоматизированную библиотечную информационную систему и электронные библиотечные системы: «Университетская библиотека ONLINE», «Электронно-библиотечная система издательства ЛАНЬ», «Электронно-библиотечная система издательства «Юрайт», «Электронно-библиотечная система IPRbooks»,«Университетская Информационная Система РОССИЯ», «Электронная библиотека диссертаций РГБ», «Научная электронная библиотека eLIBRARY», «EBSCO», «SAGE Premier». Система федеральных образовательных порталов «Экномика. Социология. Менеджмент», «Юридическая Россия», Сервер органов государственной власти РФ, Сайт Сибирского Федерального округа и др. Экран, компьютер с подключением к локальной сети филиала и выходом в Интернет, звуковой усилитель, мультимедийный проектор, столы аудиторные, стулья, трибуна, доска аудиторная. Наборы виртуального демонстрационного оборудования, наглядные учебные пособия.

Библиотека (имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет (ауд. № 101, № 102)	компьютеры с подключением к локальной сети филиала и Интернет, Wi-Fi, столы аудиторные, стулья