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

Сибирский институт управления – филиал РАНХиГС
Факультет экономики и финансов
Кафедра информатики и математики

УТВЕРЖДЕНА
кафедрой информатики и математики
Протокол от «28» августа 2018 г. № 1

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(Б1.В.ДВ.1.2)

краткое наименование дисциплины – не устанавливается

по направлению подготовки

38.04.09 Государственный аудит

направленность (профиль):

«Аудит и контроль государственных и муниципальных финансов»

квалификация выпускника: Магистр

формы обучения: заочная

Год набора – 2019

Новосибирск, 2018

Автор–составитель:
канд. техн. наук, доцент кафедры информатики и математики
С.Н. Терещенко

Заведующий кафедрой информатики и математики
канд. физ-мат. наук, доцент Е.А. Рапоцевич

СОДЕРЖАНИЕ

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

1.1. Дисциплина Б1.В.ДВ.1.2 «Информационная безопасность» обеспечивает овладение следующими компетенциями с учетом этапа:

Таблица 1

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-2	способность использовать в познавательной и профессиональной деятельности базовые знания в области основ информатики и элементы естественнонаучного и математического знания	ОПК-2.1	Способность применять основные методы количественного анализа и моделирования, теоретического и экспериментального исследования, основные способы переработки и интерпретации информации. Способность выбирать нужные информационные технологии в зависимости от исходной постановки задачи.
ОПК-11	способность к использованию в исследовательской практике математических методов, современного программного обеспечения (с учетом потребностей соответствующей области знаний)	ОПК-11.1	Способность выбирать нужные информационные технологии в зависимости от исходной постановки задачи. Способность применять основные методы количественного анализа и моделирования, теоретического и экспериментального исследования, основные способы переработки и интерпретации информации.

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

Таблица 2

Профессиональные действия	Код этапа освоения компетенции	Результаты обучения
	ОПК-2.1	на уровне знаний: основ информационной безопасности. на уровне умений: анализировать риски информационной безопасности на уровне навыков:

		навыками анализа угроз информационной безопасности
	ОПК-11.1	на уровне знаний: основ проектирования систем информационной безопасности. на уровне умений: проектировать системы информационной безопасности на уровне навыков: навыками управления в информационных системах для их безопасности;

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

- общая трудоемкость дисциплины – 3 зачётные единицы;
- количество академических часов для студентов заочной формы обучения, выделенных на контактную работу с преподавателем - 18 часов (18 час. – практических занятий), на самостоятельную работу обучающихся выделено - 86 час., на контроль – 4 часа.

Возможно изучение дисциплины по всем формам обучения с применением электронного обучения и дистанционных образовательных технологий. При этом сохраняется объем контактной и самостоятельной работы по дисциплине в соответствии с учебным планом.

Место дисциплины

Информационная безопасность (Б1.В.ДВ.1.2) изучается на 1 курсе - на заочной форме обучения.

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

Дисциплины, которые реализуются после изучения данной дисциплины: Б1.В.ДВ.5.1 Инвестиционный анализ.

3. Содержание и структура дисциплины

Таблица 3

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущ. контроля успева-емости[1], промежу-точной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам				СР	
			л	лр	пз	КСР		
Заочная форма обучения								

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

Раздел 1	Основы информационной безопасности	*34*			*8*		*26*	
Тема1.1.	Введение в информационную безопасность системы управления: использование в профессиональной деятельности базовых знаний в области основ информатики	3			1		2	О - 1.1.
Тема 1.2.	Анализ рисков и оборонительные модели организации: применение основных методов количественного анализа и моделирования	7			1		6	О – 1.2 ПЗ – 1.2
Тема 1.3.	Политика безопасности	8			2		6	О - 1.3. ПЗ – 1.3
Тема 1.4.	Аутентификация и авторизация: способы переработки и интерпретации	8			2		6	О - 1.4. ПЗ – 1.4
Тема 1.5.	Архитектура безопасности	8			2		6	О - 1.5. ПЗ – 1.5
Раздел 2	Разработка системы информационной безопасности	*70*			*10*		*60*	
Тема 2.1	Межсетевые экраны	14			2		12	О – 2.1, ПЗ – 2.1
Тема 2.2.	Системы обнаружения атак: выбор информационных технологий	14			2		12	О – 2.2, ПЗ – 2.2
Тема 2.3.	Атака и методы хакеров	14			2		12	О – 2.3, ПЗ – 2.3
Тема 2.4.	Частные виртуальные сети	14			2		12	О – 2.4, ПЗ – 2.4
Тема 2.5.	Безопасность беспроводных сетей	14			2		12	О – 2.5,
Промежуточная аттестация		4					4	Зачет
Всего:		108			18		90	ак.ч.
		3			0,5		2,5	з.е.
		81			13,5		67,5	ас.ч.

Содержание дисциплины

Раздел 1. Основы информационной безопасности

Тема 1.1. Введение в информационную безопасность системы управления: использование в профессиональной деятельности базовых знаний в области основ информатики

Понятие информационной безопасности системы управления через овладение, применение и познание в профессиональной деятельности базовых знаний в области основ информатики. 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 организации: применение основных методов количественного анализа и моделирования

Понятие рисков. Применение основных методов количественного анализа и моделирования. 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: способы переработки и интерпретации информации.

Понятие аутентификации. Средства и способы контроля аутентификации, переработки и интерпретации информации. 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: выбор информационных технологий

Выбор нужных информационных технологий в зависимости от исходной постановки задачи. 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 Б1.В.ДВ.1.2 «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: использование в профессиональной деятельности базовых знаний в области основ информатики	Устный ответ на вопросы
Тема 1.2.	Анализ рисков и оборонительные модели организации: применение основных методов количественного анализа и моделирования	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: способы переработки и интерпретации информации.	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: выбор информационных технологий	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. Промежуточная аттестация проводится в форме зачета. Зачет проводится в форме устного ответа на вопрос.

4.2. Материалы текущего контроля успеваемости обучающихся

Типовые вопросы и задания для устного (письменного) опроса

Тема 1.1. Введение в информационную безопасность системы управления: использование в профессиональной деятельности базовых знаний в области основ информатики (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: применение основных методов количественного анализа и моделирования *(О - 1.2)*

1. Понятие рисков. Основные методы количественного анализа и моделирования
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: выбор информационных технологий (О - 2.2)

1. Понятие системы обнаружения атак. Выбор нужных информационных технологий
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: применение основных методов количественного анализа и моделирования основные (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: выбор информационных технологий *(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.

Примерные темы для контрольных работ

1. VPN.
2. Алгоритм блочного шифрования DES.
3. Алгоритм шифрования с открытым ключом RSA.
4. Алгоритм электронной цифровой подписи RSA.
5. Безопасность беспроводных сетей.
6. Биометрическая идентификация и аутентификация пользователя.
7. Блочные и поточные алгоритмы шифрования.
8. Информационная безопасность в органах ГМУ.
9. Межсетевые экраны и особенности их функционирования.
10. Основные компоненты межсетевых экранов.
11. Принципы криптографической защиты информации.
12. Протокол IPsec.
13. Протокол SSL.
14. Системы обнаружения вторжений.
15. Социальный инжиниринг.
16. Средства VPN.
17. Типовые схемы идентификации и аутентификации пользователя.
18. Системы обнаружения атак: выбор информационных технологий
19. Анализ рисков и оборонительные модели организации: применение основных методов количественного анализа и моделирования
20. Основные методы количественного анализа и моделирования

4.3. Оценочные средства для промежуточной аттестации

4.3.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Таблица 5

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-2	Способность использовать в познавательной и профессиональной деятельности базовые знания в области основ информатики и элементы естественнонаучного и математического знания	ОПК-2.1	Способность применять основные методы количественного анализа и моделирования, теоретического и экспериментального исследования, основные способы переработки и интерпретации информации. Способность выбирать нужные информационные технологии в зависимости от исходной постановки задачи.
ОПК-11	способность к использованию в исследовательской практике математических методов, современного программного обеспечения (с учетом потребностей соответствующей области знаний)	ОПК-11.1	Способность выбирать нужные информационные технологии в зависимости от исходной постановки задачи. Способность применять основные методы количественного анализа и моделирования, теоретического и экспериментального исследования, основные способы переработки и интерпретации информации.

Таблица 6

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ОПК-2.1	применение основных методов количественного анализа и моделирования	умеет применять основные методы количественного анализа и моделирования
ОПК-11.1	отбор необходимых информационных технологий в зависимости от исходной постановки задачи	может проводить отбор необходимых информационных технологий в зависимости от исходной постановки задачи

4.3.2. Типовые оценочные средства

Типовые вопросы 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. Основные методы количественного анализа и моделирования
8. Сертификация средств защиты информации.
9. Политика безопасности.
10. Системы обнаружения атак: выбор информационных технологий

11. Введение в информационную безопасность системы управления: использование в профессиональной деятельности базовых знаний в области основ информатики
12. Организационные меры по защите информации.
13. Принципы криптографической защиты информации.
14. Информационная безопасность в органах ГМУ.
15. Алгоритм блочного шифрования DES.
16. Алгоритм шифрования с открытым ключом RSA.
17. Блочные и поточные алгоритмы шифрования.
18. Алгоритм электронной цифровой подписи RSA.
19. Типовые схемы идентификации и аутентификации пользователя.
20. Биометрическая идентификация и аутентификация пользователя.
21. Протокол SSL.
22. Центры сертификации.
23. Понятие о типах вирусов и способы защиты.
24. Защита от троянских программ.
25. Защита электронной почты.
26. Защита локальной рабочей станции.
27. Защита локальной сети.
28. Межсетевые экраны и особенности их функционирования.
29. Основные компоненты межсетевых экранов.
30. Системы обнаружения вторжений.
31. Управление журналами и оповещениями.
32. Методы хакеров.
33. Атаки на отказ в обслуживании.
34. Распределенные атаки.
35. Переполнение буфера.
36. Снифферы и спуфферы.
37. SQL-инъекции.
38. Социальный инжиниринг.
39. VPN.
40. Протокол IPsec.
41. Средства VPN.
42. Безопасность беспроводных сетей.
43. Технологии взлома беспроводных сетей.

.

Шкала оценивания

Таблица 7

Зачет (балл)	Критерии оценки
Незачтено (0-50)	Студент демонстрирует фрагментарные знания учебного материала, не может проводить анализ фактов, событий, явлений, а также применять основные методы количественного анализа и моделирования, может проводить отбор необходимых информационных технологий в зависимости от исходной постановки задачи.
зачтено (51-100)	Студент демонстрирует свободное владение материалом, понятийным аппаратом дисциплины, умеет самостоятельно проводить анализ фактов, событий, явлений, умеет применять основные методы количественного анализа и моделирования, может проводить отбор необходимых информационных технологий в зависимости от исходной постановки задачи.

4.4. Методические материалы промежуточной аттестации

Зачет включает ответы на два теоретических вопроса.

Ответы на теоретические вопросы даются в устной форме.

Для получения зачета необходимо изучить рекомендуемую основную литературу, а также усвоить умения и навыки в ходе контактной работы с преподавателем путем опроса и выполнения различных практических заданий на компьютере.

Студент при подготовке к ответу по билету формулирует ответ на вопрос, а также выполняет задание на компьютере.

При подготовке ответов на вопросы стоит использовать соответствующий дисциплине понятийный аппарат, отвечать с пояснениями, полно и аргументированно.

При сравнении явлений необходимо представить аргументы, представляющие их сходства и различия. Давать односложные ответы нежелательно.

При ответе студент должен полно и аргументированно ответить на вопрос билета, демонстрируя знания либо умения в его рамках.

Итоговая оценка по дисциплине формируется по результатам выполнения ПКЗ и прохождения экзамена на основании следующей формулы:

Σ = УО х 0,5 + УО х 0,5

ТИПОВЫЕ БИЛЕТЫ К ЗАЧЕТУ

Билет 1.
Вопрос: Политика безопасности.
Вопрос: Методы хакеров.

Билет 2.
Вопрос: SQL-инъекции.
Вопрос: Безопасность беспроводных сетей.

Ответ на вопросы билета оценивается по системе зачет/незачет.

При дистанционном формате изучения дисциплины промежуточная аттестация может проводиться в формате тестирования, выполнения письменного контрольного задания или опроса по вопросам билета или защиты выполненной работы в режиме онлайн видеоконференций. Все вопросы и задания, выносимые на промежуточную аттестацию, находятся в рамках тематического содержания дисциплины, представленного в РПД. Прокторинг является обязательным при проведении промежуточной аттестации с использованием ЭО и ДОТ.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

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

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

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 по написанию контрольной работы

Контрольная работа выполняется в форме аналитической работы. Тема работы выбирается из рекомендованного списка или по предложению студента с согласия преподавателя дисциплины. Она формулируется конкретно.

Написание контрольной работы может быть посвящено как общим вопросам методологии, методики и практики проведения экспертно-аналитических мероприятий, так и конкретным вопросам. Контрольная работа может содержать теоретический и аналитический разделы.

Контрольная работа состоит из 5 основных частей:

- введения,
- теоретическая часть,
- аналитическая часть,
- заключения,
- списка использованной литературы (15 источников).

Во введении раскрывается значение и актуальность выбранной темы, определяется место проблемы в системе финансово-экономических знаний. Ставится цель и/или задачи.

В теоретическом разделе рассматриваются вопросы методологии и методики исследования анализируемой проблемы, в аналитической части – анализ исследуемой темы на основе конкретных статистических данных и актуальной нормативно-правовой базы, формулируются предложения по решению выявленной проблемы на основе имеющейся или развитой автором методической базе. В заключении формулируются краткие выводы по изложенному материалу, и приводится собственная точка зрения на представленные в работе проблемы. Заключение имеет форму синтеза полученных в работе результатов.

Объем контрольной работы 20 страниц. Гарнитура Times New Roman, интервал 1,5, размер шрифта 14.

Во время проведения экзамена студентам запрещается иметь при себе и использовать средства связи. Использование материалов, а также попытка общения с другими студентами или иными лицами, в том числе с применением электронных средств

связи, несанкционированные перемещения и т.п. являются основанием для удаления студента из аудитории и последующего проставления оценки «неудовлетворительно».

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.

При применении дистанционной технологии обучения по очной, очно-заочной, заочной (традиционной) форм обучения учебный материал[2], который необходимо обучающимся проработать по конкретной лекции размещается в СДО «Прометей». Все обучающиеся имеют доступ в СДО «Прометей» из личного кабинета студента через сайт Сибирского института управления – филиала РАНХиГС.

Дополнительно, при наличии технической возможности, лекционные занятия могут проводятся в соответствии с расписанием в режиме онлайн видеоконференций, для организации которых используются сервисы Zoom, Microsoft Teams, Youtube. В СДО «Прометей» для обучающихся заранее размещаются соответствующие ссылки и идентификаторы конференции. Может быть использована синхронная или асинхронная аудио/видео-конференция посредством вебинара.

Для контроля освоения темы обучающимся выдаются вопросы и задания в соответствии с РПД. Задания размещаются в СДО «Прометей» и /или доводятся до обучающегося любым доступным способом (посредством электронной почты, соц. сетей и др.). Устанавливается срок выполнения и представления заданий, в том числе способ представления.

Материалы, предназначенные для обеспечения семинарских/практических занятий размещаются в СДО «Прометей» и /или доводятся до обучающегося любым доступным способом (посредством электронной почты, соц сетей и др.). в привязке к конкретным занятиям, запланированным в учебном расписании это:

вопросы для обсуждения на семинарских занятиях, планы практических занятий, материалы для подготовки к ним;

тестовые материалы, привязанные к конкретному занятию и предназначенные для автоматической оценки степени освоения обучающимся материалов темы;

варианты письменных работ и методических указаний по их выполнению.

По каждой теме преподаватель осуществляет оперативное консультирование обучающихся, отвечая письменно на их вопросы в СДО «Прометей» и /или в формате чатов в процессе аудио/видео-конференций.

[2] Материалы конкретных лекционных занятий, с которыми должен ознакомиться обучающийся в рамках данной «лекции»: текст (конспект) лекции, демонстрационные и дополнительные материалы к ним (презентации, учебные фильмы или ссылки на них, материалы для чтения: статьи, документы, хрестоматийный материал), включая ЭБС, ссылки на публичные онлайн-курсы и т.п. с указанием конкретных страниц учебников, конспекта, отрезков видео или фрагментов онлайн-курса, которые должен освоить обучающийся в рамках данного «лекционного» занятия.

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

6.1. Основная литература

1. Внуков, А. А. Защита информации [Электронный ресурс] : учеб. пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Электрон. дан. — Москва : Издательство Юрайт, 2016. — 261 с. — Доступ из ЭБС изд-ва «Юрайт». — Режим доступа : https://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1, требуется авторизация. — Загл. с экрана.

2. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учеб. и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — Электрон. дан. — Москва : Издательство Юрайт, 2016. — 325 с. — Доступ из ЭБС изд-ва «Юрайт». — Режим доступа : https://www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847, требуется авторизация. — Загл. с экрана.

6.2. Дополнительная литература

1. Анисимов, А. А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А. А. Анисимов. — Электрон. дан. — Москва : ИНТУИТ, 2016. — 212 с. — Доступ из ЭБС «IPRbooks». - Режим доступа : http://www.iprbookshop.ru/52182, требуется авторизация. - Загл. с экрана.

2. 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. – 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. — Загл. с экрана.

3. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие [для студентов, аспирантов и специалистов] / 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. - Загл. с экрана.

4. Безопасность систем баз данных [Электронный ресурс] : учеб. пособие / А. В. Скрыпников [и др.]. — Электрон. дан. — Воронеж : Воронеж. гос. ун-т инженер. технологий, 2015. — 144 с. — Доступ из ЭБС «IPRbooks». - Режим доступа : http://www.iprbookshop.ru/50628, требуется авторизация. — Загл. с экрана.

5. Галатенко, В. А. Основы информационной безопасности [Электронный ресурс] / В. А. Галатенко. – Электрон. дан. - Москва : ИНТУИТ, 2016. — 266 с. — Доступ из ЭБС «IPRbooks». - Режим доступа : http://www.iprbookshop.ru/52209, требуется авторизация. – Загл. с экрана.

6. Загинайлов, Ю. Н. Основы информационной безопасности [Электронный ресурс] : курс визуальных лекций : учеб. 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. — Загл. с экрана.

7. Инструментальный контроль и защита информации [Электронный ресурс] : учеб. пособие / Н. А. Свинарев, О. В. Ланкин, А. П. Данилкин и др. ; Воронеж. гос. ун-т инженер. технологий. - Электрон. дан. – Воронеж : Воронеж. гос. ун-т инженерных технологий, 2013. - 192 с. - Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=255905, требуется авторизация. — Загл. с

экрана. - То же [Электронный ресурс]. — Доступ из ЭБС «IPRbooks». — Режим доступа : http://www.iprbookshop.ru/47422, требуется авторизация. — Загл. с экрана.

8. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / С. А. Нестеров ; С.-Петерб. гос. политехн. ун-т. - Электрон. дан. – Санкт-Петербург : Изд-во Политехн. ун-та, 2014. - 322 с. - Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=363040, требуется авторизация. — Загл. с экрана. - То же [Электронный ресурс]. — Доступ из ЭБС «IPRbooks». — Режим доступа : http://www.iprbookshop.ru/43960, требуется авторизация. — Загл. с экрана.

9. 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. — Загл. с экрана.

10. 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. — Загл. с экрана.

11. 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. — Загл. с экрана.

6.3. Учебно-методическое обеспечение самостоятельной работы

1. Терещенко, С. Н. Информационная безопасность компьютерных систем : учеб. пособие для студентов всех форм обучения по специальности 080504.65 - Гос. и муницип. упр., специализации "Информ. технологии в гос. и муницип. упр." / С. Н. Терещенко ; Федер. агентство по образованию, Сиб. акад. гос. службы. - Новосибирск : Изд-во СибАГС, 2010. - 170 с. - То же [Электронный ресурс]. - Доступ из Б-ки электрон. изд. / Сиб. ин-т упр. – филиал РАНХиГС. – Режим доступа : http://www.sapanet.ru, требуется авторизация. - Загл. с экрана.

6.4. Нормативные правовые документы

1. О внедрении защищенного электронного документооборота в целях реализации законодательства Российской Федерации об обязательном пенсионном страховании, (вместе с «Регламентом обмена документами по телекоммуникационным каналам связи в системе электронного документооборота Пенсионного фонда Российской Федерации», «Регламентом обеспечения безопасности информации при защищенном обмене электронными документами в системе электронного документооборота Пенсионного фонда Российской Федерации по телекоммуникационным каналам связи) : Распоряжение Правления ПФ РФ от 11.10.2007 № 190р // КонсультантПлюс [Электронный ресурс] : офиц. сайт / Компания «КонсультантПлюс». – Электрон. дан. – М., 1997 – 2012. – Режим доступа.: http://www.consultant.ru, свободный из локальной сети Сиб. ин-та управления РАНХиГС.

2. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // КонсультантПлюс [Электронный ресурс] : офиц. сайт / Компания «КонсультантПлюс». – Электрон. дан. – М., 1997 – 2012. – Режим доступа.: http://www.consultant.ru, свободный из локальной сети Сиб. ин-та управления РАНХиГС.

6.5. Интернет-ресурсы

1. ЭОС: Системы электронного документооборота. Компания ЭОС - ведущий разработчик систем управления документооборотом, электронными и бумажными архивами, бизнес-процессами и корпоративным контентом, лидер рынка СЭД/ECM-систем России и стран СНГ [Электронный ресурс] – Режим доступа: http://www.eos.ru, свободный. — Загл. с экрана.
2. КонсультантПлюс - надёжная правовая поддержка [Электронный ресурс] : офиц. сайт / Компания «КонсультантПлюс». – Электрон. дан. – М., 1997 – 2012. – Режим доступа.: http://www.consultant.ru, свободный из локальной сети Сиб. ин-та управления РАНХиГС.
3. 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. (дата обращения: 19.01.2015).
4. 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

6.6. Иные источники

Иные источники не используются.

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

7.1. Программное обеспечение, необходимое для реализации учебного процесса по дисциплине, включают в себя: Microsoft Windows, Microsoft Office, сайт филиала, СДО Прометей, корпоративные базы данных, СУБД MS SQL (2008 и выше), MS Visual Studio (2010 и выше).

7.2. Технические средства и материально-техническое обеспечение дисциплины

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебные аудитории для проведения занятий лекционного типа	Экран, компьютер с подключением к локальной сети института, и выходом в Интернет, звуковой усилитель, антиподавитель, мультимедийный проектор, столы аудиторные, стулья, трибуна настольная, доска аудиторная
Класс деловых игр	Ноутбуки, выход в Интернет ч/з Wi-Fi, аудиторная доска, аудиторные столы, стулья
Учебные аудитории для проведения занятий семинарского типа	Интерактивная доска (экран), компьютер с подключением к локальной сети филиала и выходом в Интернет, звуковой усилитель, антиподавитель, мультимедийный проектор, столы аудиторные, стулья, трибуна настольная, доска аудиторная
Лаборатория личностного и профессионального развития	Экран, компьютер с подключением к локальной сети института, и выходом в Интернет, мультимедийный проектор, столы аудиторные, стулья, трибуна настольная, доска аудиторная

Помещения для самостоятельной работы обучающихся. Компьютерные классы. Центр интернет-ресурсов	Компьютерные классы: компьютеры с подключением к локальной сети института (включая правовые системы) и Интернет, программа 1С, столы аудиторные, стулья, доски аудиторные. Центр интернет-ресурсов: компьютеры 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	Компьютеры с подключением к локальной сети филиала и Интернет, Wi-Fi, столы аудиторные, стулья, Wi-Fi
Специализированный кабинет для занятий с маломобильными группами (студенты с ограниченными возможностями здоровья)	Экран, компьютеры с подключением к локальной сети института и выходом в Интернет, звуковой усилитель, мультимедийный проектор, столы аудиторные, стулья, трибуна настольная, доска аудиторная, офисные кресла
Видеостудия для вебинаров	компьютеры с выходом в Интернет, оснащенные веб-камерами и гарнитурами (наушники+микрофон), столы, стулья