

Сибирский институт управления – филиал РАНХиГС
Факультет государственного и муниципального управления
Кафедра информатики и математики

УТВЕРЖДЕНА
кафедрой информатики и
математики
Протокол от 29.08.2017г. №1

**РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(Б1.В.ДВ.5.1)

не устанавливается

краткое наименование дисциплины

по направлению подготовки: 38.03.04 Государственное муниципальное
управление

направленность (профиль): «Информационные технологии в
государственном и муниципальном управлении»

квалификация выпускника: Бакалавр

форма обучения: очная

Год набора – 2018

Новосибирск, 2017

Автор – составитель, заведующий кафедрой ИиМ, доцент, к.ф.-м.н. Е. А. Рапоцевич

СОДЕРЖАНИЕ

1	Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы	4
2.	Объем и место дисциплины в структуре ОП ВО	5
3.	СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ	6
4.	Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине	11
5.	МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	18
6.	Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине	20
7.	Материально – техническая база, информационные технологии, программное обеспечение и информационные справочные системы	23

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

1.1. Дисциплина (Б1.В.ДВ.5.3) «Информационная безопасность» обеспечивает овладение следующими компетенциями с учетом этапа:

Таблица 1.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-26	владение навыками сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций	ПК-26.3	Способность осознавать сущность и значимость информации в современном обществе

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

Таблица 2.

Профессиональные действия	Код этапа освоения компетенции	Результаты обучения
собирать, анализировать и структурировать информацию, необходимую для деятельности органов публичной власти	ПК-26.3	<p>на уровне знаний: знать роль и место обеспечения информационной безопасности при информатизации деятельности органа власти</p> <p>на уровне умений: уметь анализировать риски и угрозы информационной безопасности, разрабатывать политику и систему информационной безопасности при проведении информатизации органа власти</p> <p>на уровне навыков: современными средствами обеспечения информационной безопасности информационных сетей органа власти</p>

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Количество академических часов, выделенных на контактную работу с преподавателем.

очная форма обучения

- 56 часов (18 часа лекций, 38 часа практических (семинарских) занятий);
на самостоятельную работу обучающихся – 16 часов.

очно-заочная форма обучения

- 18 часов (8 часов лекций, 10 часов практических (семинарских) занятий);
на самостоятельную работу обучающихся – 54 часа.

заочная форма обучения

- 8 часов (4 часа лекций, 4 часа практических (семинарских) занятий);
на самостоятельную работу обучающихся – 60 час.

заочная форма обучения с применением ЭО, ДОТ

- 8 часов (4 часа лекций, 4 часа практических (семинарских) занятий);
на самостоятельную работу обучающихся – 60 час.

Место дисциплины

Информационная безопасность (Б1.В.ДВ.5.3) изучается на 3 курсе (6 семестр) очной формы обучения, в 8 семестре очно-заочной формы, 5 семестре заочной формы обучения и заочной формы обучения с применением ЭО, ДОТ.

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.В.ДВ.7.3 Информационные системы в делопроизводстве и кадровой работе.

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		
<i>Очная форма обучения</i>								
Раздел 1	Основы информационной безопасности	32	8		16		8	
Тема 1.1.	Введение в информационную	4	1		2		1	О - 1.1.
Тема 1.2.	Анализ рисков и оборонительные модели организации	8	2		4		2	О – 1.2 ПЗ – 1.2
Тема 1.3.	Политика безопасности	4	1		2		1	О - 1.3. ПЗ – 1.3
Тема 1.4.	Аутентификация и авторизация	8	2		4		2	О - 1.4. ПЗ – 1.4
Тема 1.5.	Архитектура безопасности	8	2		4		2	О - 1.5. ПЗ – 1.5
Раздел 2	Разработка системы информационной безопасности	40	10		20		10	
Тема 2.1	Межсетевые экраны	8	2		4		2	О – 2.1, ПЗ – 2.1
Тема 2.2.	Системы обнаружения атак	8	2		4		2	О – 2.2, ПЗ – 2.2
Тема 2.3.	Атака и методы хакеров	8	2		4		2	О – 2.3, ПЗ – 2.3
Тема 2.4.	Частные виртуальные сети	8	2		4		2	О – 2.4, ПЗ – 2.4
Тема 2.5.	Безопасность беспроводных сетей	8	2		4		2	О – 2.5,
Промежуточная аттестация								Зачет
Всего:		72	18		38		16	ак. ч
		2						з.е.
		54						ас.ч.

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

Таблица 4.

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.					СР	Форма текущ. контроля успеваемости ² , промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий					
			л	лр	пз	КСР		
<i>Очно-заочная форма обучения</i>								
Раздел 1	Основы информационной безопасности	28	4		4		20	
Тема 1.1.	Введение в информационную							О - 1.1.
Тема 1.2.	Анализ рисков и оборонительные модели организации							О – 1.2 ПЗ – 1.2
Тема 1.3.	Политика безопасности							О - 1.3. ПЗ – 1.3
Тема 1.4.	Аутентификация и авторизация							О - 1.4. ПЗ – 1.4
Тема 1.5.	Архитектура безопасности							О - 1.5. ПЗ – 1.5
Раздел 2	Разработка системы информационной безопасности	44	4		6		34	
Тема 2.1	Межсетевые экраны							О – 2.1, ПЗ – 2.1
Тема 2.2.	Системы обнаружения атак							О – 2.2, ПЗ – 2.2
Тема 2.3.	Атака и методы хакеров							О – 2.3, ПЗ – 2.3
Тема 2.4.	Частные виртуальные сети							О – 2.4, ПЗ – 2.4
Тема 2.5.	Безопасность беспроводных сетей							О – 2.5,
Промежуточная аттестация								Зачет
Всего:		72	8		10		54	ак. ч
		2						з.е.
		54						ас.ч.

² Формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), практические задания (ПЗ)

Таблица 5.

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.					Форма текущ. контроля успеваемости ³ , промежуточной аттестации	
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий					СР
			л	лр	пз	КСР		
<i>заочная форма обучения</i>								
Раздел 1	Основы информационной безопасности	24	2		2		20	
Тема 1.1.	Введение в информационную						О - 1.1.	
Тема 1.2.	Анализ рисков и оборонительные модели организации						О – 1.2 ПЗ – 1.2	
Тема 1.3.	Политика безопасности						О - 1.3. ПЗ – 1.3	
Тема 1.4.	Аутентификация и авторизация						О - 1.4. ПЗ – 1.4	
Тема 1.5.	Архитектура безопасности						О - 1.5. ПЗ – 1.5	
Раздел 2	Разработка системы информационной безопасности	44	2		2		40	
Тема 2.1	Межсетевые экраны						О – 2.1, ПЗ – 2.1	
Тема 2.2.	Системы обнаружения атак						О – 2.2, ПЗ – 2.2	
Тема 2.3.	Атака и методы хакеров						О – 2.3, ПЗ – 2.3	
Тема 2.4.	Частные виртуальные сети						О – 2.4, ПЗ – 2.4	
Тема 2.5.	Безопасность беспроводных сетей						О – 2.5,	
Промежуточная аттестация		4				2	2	Зачет
Всего:		72	4		4	2	62	ак. ч
		2						з.е.
		54						ас.ч.

Таблица 6.

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.	Форма текущ.
-------	-----------------------------	------------------------	--------------

³ Формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), практические задания (ПЗ)

		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	контроля успеваемости ⁴ , промежуточной аттестации
			л/эо, дог ⁵	лр/э, дог ⁶	пз/э, дог ⁷	КСР		
заочная форма обучения с применением ЭО, ДОТ								
Раздел 1	Основы информационной безопасности	24	2		2		20	
Тема 1.1.	Введение в информационную						Электронный семинар	
Тема 1.2.	Анализ рисков и оборонительные модели организации							
Тема 1.3.	Политика безопасности							
Тема 1.4.	Аутентификация и авторизация							
Тема 1.5.	Архитектура безопасности							
Раздел 2	Разработка системы информационной безопасности	44	2		2		40	
Тема 2.1	Межсетевые экраны						Электронный семинар	
Тема 2.2.	Системы обнаружения атак							
Тема 2.3.	Атака и методы хакеров							
Тема 2.4.	Частные виртуальные сети							
Тема 2.5.	Безопасность беспроводных сетей							
Промежуточная аттестация						2	2	Зачет
Всего:		72	4		4	2	62	ак. ч
		2						з.е.
		54						ас.ч.

⁴ Формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), практические задания (ПЗ)

⁵ При применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом

⁶ При применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом

⁷ При применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом

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 (Б1.В.ДВ.5.3) «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 7.

Для проведения занятий по очной, очно-заочной и заочной формам обучения

Тема (раздел)		Методы текущего контроля успеваемости
Раздел 1	Основы информационной безопасности	
Тема 1.1.	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 с применением следующих методов (средств):

устное собеседование по вопросам билета либо письменные ответы на вопросы билета (очная и заочная формы обучения); письменная работа и компьютерное тестирование (заочная форма обучения с применением ЭО и ДОТ). Выбор метода оценивания для традиционной формы обучения осуществляет преподаватель, информируя обучающихся в день проведения консультации к экзамену.

4.2. Материалы текущего контроля успеваемости обучающихся

Полный перечень материалов текущего контроля находится на кафедре Информатики и математики.

ТИПОВЫЕ ВОПРОСЫ И ЗАДАНИЯ ДЛЯ 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 С#, имитирующее атаку доступа.
2. Создайте программное обеспечение на С#, 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.

Электронный семинар

Типовые вопросы электронного семинара к разделу 1

Перечислите основные положения законодательства, регламентирующие деятельность в сфере информационной безопасности.

Типовые вопросы электронного семинара к разделу 2

Назовите основные компоненты защиты информационной безопасности.

4.3. Оценочные средства 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 8.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-26	владение навыками сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций	ПК-26.3	Способность осознавать сущность и значимость информации в современном обществе

Таблица 9.

Очная форма, очно-заочная, заочная форма, заочная форма с ЭО и ДОТ

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ПК-26.3 Способность осознавать сущность и значимость информации в современном обществе	Может ориентироваться в основных информационных процессах. Знает принципы использования современных информационных технологий и инструментальных средств для решения различных задач своей профессиональной деятельности.	Использует методы решения экономических задач с помощью ИС. Работает с современными программными средствами.

4.3.2. Типовые оценочные средства

Полный перечень вопросов и заданий находится на кафедре информатики и математики.

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.

ТИПОВОЙ ВАРИАНТ ПИСЬМЕННОГО КОНТРОЛЬНОГО ЗАДАНИЯ (ПКЗ)

(для заочной формы обучения с применением ЭО и ДОТ)

Разработайте основные положения политики информационной безопасности для организации, в которой работаете.

Таблица 10.

Очная, очно-заочная, заочная форма и заочная форма с ЭО и ДОТ

Зачет (балл)	Критерии оценки
Незачтено (0-50)	Этапы компетенции, 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..

Зачет (балл)	Критерии оценки
Зачтено (51-100)	<p>Свободно ориентируется в вопросах обеспечения информационной безопасности при информатизации деятельности организации. Этапы компетенции, предусмотренные образовательной программой, сформированы на высоком уровне.</p> <p>Умеет анализировать риски и угрозы информационной безопасности, разрабатывать политику и систему информационной безопасности при проведении информатизации организации. Практические навыки профессиональной деятельности сформированы на высоком уровне. Способность к самостоятельному нестандартному решению практических задач.</p>

4.4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Зачет включает ответы на теоретические вопросы и выполнение практических заданий.

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

Выполнение практических заданий проводится в письменной форме.

Студент при подготовке к ответу по билету формулирует ответ на вопрос, а также выполняет задание (письменно либо устно, в зависимости от содержания задания).

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

При выполнении задания необходимо четко определить его суть и необходимый результат его выполнения. При решении практического задания необходимо определить тему, основную формулу в теме и записать данные задачи в терминах курса. Это позволит определить неизвестную величину и решить задачу.

При демонстрации выполненного задания студент должен аргументировать свое решение (формулировку текста и т.д.), демонстрируя знания, умения либо навыки в полной мере.

Ответ на каждый вопрос (задание) билета оценивается по шкале «зачтено/незачтено» в соответствии со шкалой оценивания.

Для студентов, обучающихся на заочной форме обучения с применением ЭО и ДОТ выполнение письменного контрольного задания позволяет оценить умения и навыки по дисциплине и осуществляется в течении семестра.

Проверка знаний также осуществляется с помощью тестовых заданий. Тестирование проводится в СДО "Прометей" в соответствии с установленными требованиями. Итоговый тест формируется на аппаратном уровне с использованием банка тестовых заданий по дисциплине. Проверка результатов тестирования осуществляется автоматически.

Алгоритм расчета итоговой оценки студентов, обучающихся на заочной форме обучения с применением ЭО и ДОТ, установлен «Регламентом о системе оценивания знаний обучающихся по дисциплинам учебного модуля по образовательным программам с применением электронного обучения на факультете заочного и дистанционного обучения Сибирского института управления-филиала РАНХиГС».

Для обучающихся, с ограниченными возможностями здоровья и в соответствии с медицинскими показаниями, зачет может быть проведен в устной (письменной) форме по согласованию с преподавателем.

Студент обязан явиться на зачет в указанное в расписании время. Опоздание на зачет не допускается. В порядке исключения на зачет могут быть допущены лица, предъявившие оправдательные документы, связанные с причинами опоздания.

Во время проведения зачета 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 «незачет».

Семинарские занятия студентов всех форм обучения проводятся в компьютерных классах.

ТИПОВЫЕ БИЛЕТЫ К ЗАЧЕТУ

Билет 1.

Вопрос: Политика безопасности.

Билет 2.

Вопрос: SQL-инъекции.

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

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания для обучающихся по очной форме обучения

Студентам рекомендуется вести две специальные тетради: для записи основных положений лекций (конспектов) и для самостоятельной работы при подготовке к практическим занятиям.

Студент обязательно должен посетить первые лекции, на которых излагается цель, задачи и содержание курса, поясняются контрольные точки балльно-модульной системы, приводятся рекомендации и критерии оценивания.

Для наилучшего усвоения материала студенту рекомендуется посещать все лекционные и семинарские занятия, что будет способствовать постепенному накоплению знания, максимальному развитию умений и навыков. Кроме того, студенту рекомендуется выполнять все виды самостоятельной работы.

К каждой теме семинара студент выполняет домашнее задание по пройденной теме, которое проверяется и разбирается в начале каждого следующего семинара.

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

Методические указания для обучающихся по заочной форме обучения:

Особенностью освоения данной дисциплины по заочной форме является минимизация устных форм опроса и выполнения практических заданий из-за небольшого объема аудиторных занятий. Основным методом обучения на заочной форме выступает собственно самостоятельная работа, которая выполняется индивидуально в произвольном режиме времени в удобные для обучающегося часы, часто вне аудитории - внеаудиторная самостоятельная работа.

Рекомендации для студентов заочной формы обучения с применением ЭО, ДОТ изложены в «Методических рекомендациях по освоению дисциплины «Информационная безопасность» студентами заочной формы обучения с применением ЭО, ДОТ», которые размещены на сайте Сибирского института управления – филиала РАНХиГС <http://siu.ranepa.ru/sveden/education/>

Методические рекомендации для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья имеют возможность изучать дисциплину по индивидуальному плану, согласованному с преподавателем и деканатом.

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием средств обучения общего и специального назначения.

При освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья по индивидуальному плану предполагаются: индивидуальные консультации с преподавателем (разъяснение учебного материала и углубленное изучение материала), индивидуальная самостоятельная работа.

В процессе обучения студентам из числа инвалидов и лиц с ограниченными возможностями здоровья информация предоставляется в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушением зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа (с возможностью увеличения шрифта).

В случае необходимости информация может быть представлена в форме аудиофайла.

Для лиц с нарушением слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушением опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Индивидуальные консультации с преподавателем проводятся по отдельному расписанию, утвержденному заведующим кафедрой (в соответствии с индивидуальным графиком занятий обучающегося).

Индивидуальная самостоятельная работа обучающихся проводится в соответствии с рабочей программой дисциплины и индивидуальным графиком занятий.

Текущий контроль по дисциплине осуществляется в соответствии с фондом оценочных средств, в формах, адаптированных к ограничениям здоровья и восприятия информации обучающихся.

Методические указания по проведению опроса

Устный опрос - наиболее распространенный метод контроля знаний студентов. При устном контроле устанавливается непосредственный контакт между преподавателем и студентом, в процессе которого преподаватель получает широкие возможности для изучения индивидуальных особенностей усвоения студентами учебного материала.

Для организации коллективной работы группы во время индивидуального опроса преподаватель может дать задание, такое как приведение примеров по тому или иному положению ответа.

Если отвечающий не в состоянии понять и поправить ошибку, преподаватель вызывает другого студента для ее исправления. В необходимых случаях целесообразно направляющими ответами помогать СТУДЕНТУ, не показывая ему правильного ответа.

Длительность устного опроса зависит от темы занятия, ее сложности, вида занятий, индивидуальных особенностей студентов.

Заключительная часть устного опроса — подробный анализ ответов студентов. Преподаватель отмечает положительные стороны, указывает на положительные стороны, указывает на недостатки ответов, делает выводы о том, как изучен учебный материал. При оценке ответа учитывают его правильность и полноту, сознательность, логичность изложения материала, культуру речи, умение увязывать теоретические положения с практикой, в том числе и с будущей профессиональной деятельностью.

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 : 02.08.2016). — 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 : 19.07.2016). — Загл. с экрана.
2. 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 : 09.08.2016). - Загл. с экрана.
3. 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 : Юрайт, 2017. — 261 с. — Доступ из ЭБС изд-ва «Юрайт». — Режим доступа : <https://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1>, требуется авторизация (09.08.2016). — Загл. с экрана.
4. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / С. А. Нестеров ; Санкт-Петерб. гос. политехн. ун-т. - 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 : 19.07.2016). — Загл. с экрана. - То же [Электронный ресурс]. — Доступ из ЭБС «IPRbooks». — Режим доступа : <http://www.iprbookshop.ru/43960>, требуется авторизация (дата обращения : 19.07.2016). — Загл. с экрана.

6.2. Дополнительная литература

1. Басалова, Г. В. Основы криптографии [Электронный ресурс] / Г. В. Басалова. — Электрон. дан. — Москва : ИНТУИТ, 2016. — 282 с. — Доступ из ЭБС «IPRbooks». — Режим доступа : <http://www.iprbookshop.ru/52158>, требуется авторизация (дата обращения : 19.07.2016). — Загл. с экрана.
2. 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 : 19.07.2016). — Загл. с экрана.
3. 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 (дата обращения : 09.07.2016). – Загл. с экрана.

4. 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 (дата обращения : 19.07.2016). — Загл. с экрана.

5. Кияев, В. Безопасность информационных систем [Электронный ресурс] : курс / В. Кияев, О. Граничин. - Электрон. дан. – Москва : 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 : 19.07.2016). — Загл. с экрана.

6. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учеб. и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. [и др.] ; под ред. Т. А. Поляковой, А. А. Стрельцова. — Электрон. дан. — Москва : 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 (дата обращения : 08.08.2016). — Загл. с экрана.

7. Организация безопасной работы информационных систем [Электронный ресурс] : учеб. пособие / Ю. Ю. Громов, Ю. Ф. Мартемьянов, Ю. К. Букурако и др. ; Тамбов. гос. техн. ун-т. - Электрон. дан. – Тамбов : 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 : 19.07.2016). — 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 : 19.07.2016). — Загл. с экрана.

9. Технологии защиты информации в компьютерных сетях [Электронный ресурс] / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суоров. - 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 : 09.07.2016). — Загл. с экрана.

10. 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 : 19.07.2016). — 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

Таблица 11.

Наименование специальных помещений и помещений для самостоятельной работ	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
Учебные аудитории для проведения занятий семинарского типа	Компьютерные классы: компьютеры с подключением к локальной сети института (включая правовые системы) и Интернет, столы аудиторные, стулья, доски аудиторные.
Аудитория для самостоятельной работы обучающихся. Интернет-ресурсы Центр	Мультимедийный проектор, Экран проекционный, Принтер, ПК, с подключенным интернетом и к локальной сети института (включая правовые системы) и Интернет, 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 «Экономика. 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

Видеостудия для проведения вебинаров	Два рабочих места, оснащенных компьютерами, веб-камерами и гарнитурам (наушники и микрофон).
Видеостудия для вебинаров	Два рабочих места, оснащенных компьютерами, веб-камерами и гарнитурам (наушники и микрофон).
Кафедры	На каждой кафедре одно рабочее место, оснащенное компьютером, веб-камерой, гарнитурой.