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

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

УТВЕРЖДЕНА
кафедрой информатики и математики
Протокол от «26» августа 2016 г. №1

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(Б1.В.ДВ.5.3)

краткое наименование дисциплины – не устанавливается

по направлению подготовки: 38.03.04 Государственное муниципальное управление

направленность (профиль): «Административно-государственное управление»

квалификация: Бакалавр

формы обучения: очная, очно-заочная, заочная

Год набора - 2017

Новосибирск, 2016

Автор–составитель:
к.т.н., доцент, доцент кафедры информатики и математики
Терещенко С.Н.

Заведующий кафедрой информатики и математики:
к.ф.-м.н, доцент Рапоцевич Е. А.

СОДЕРЖАНИЕ

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 на очной, очно-заочной, заочной, формам обучения ПК – 26.2 заочной с применением ЭО, ДОТ форме обучения	Способность осознавать сущность и значимость информации в современном обществе Способность к информатизации деятельности соответствующих органов власти и организаций

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

Таблица 2.

ОТФ/ТФ	Код этапа освоения компетенции	Результаты обучения
собирать, анализировать и структурировать информацию, необходимую для деятельности органов публичной власти	ПК-26.3 на очной, очно-заочной, заочной, формам обучения заочной с применением ЭО, ДОТ	на уровне знаний: -понятие, виды, основные способы сохранения и использования информации, ее роль в развитии человеческого общества; -знать роль и место обеспечения информационной безопасности при информатизации деятельности органа власти на уровне умений: уметь анализировать риски и угрозы информационной безопасности, на уровне навыков: -способами оценки информации и пониманием сущности когнитивных процессов; -навыками использования современных средств обеспечения информационной безопасности информационных сетей органа власти;

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 – 60 часов.

заочная форма обучения

- 8 часов (4часа лекций, 4 часа практических (семинарских) занятий);

на самостоятельную работу обучающихся – 60 часов.

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.

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.

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				СР	
			л	лр	пз	**КСР**		
Очная форма обучения								
Раздел 1	**Основы информационной безопасности**	**32**	**8**		**16**		**8**	
Тема1.1.	Введение в информационную	4	1		2		1	О
Тема 1.2.	Анализ рисков и оборонительные модели организации	8	2		4		2	О ПЗ

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

Тема 1.3.	Политика безопасности	4	1		2		1	О ПЗ
Тема 1.4.	Аутентификация и авторизация	8	2		4		2	О ПЗ
Тема 1.5.	Архитектура безопасности	8	2		4		2	О ПЗ
Раздел 2	**Разработка системы информационной**	**40**	**10**		**20**		**10**	
Тема 2.1	Межсетевые экраны	8	2		4		2	О ПЗ
Тема 2.2.	Системы обнаружения атак	8	2		4		2	О ПЗ
Тема 2.3.	Атака и методы хакеров	8	2		4		2	О ПЗ
Тема 2.4.	Частные виртуальные сети	8	2		4		2	О ПЗ
Тема 2.5.	Безопасность беспроводных сетей	8	2		4		2	О
Промежуточная аттестация								Зачет
Всего:		**72**	**18**		**38**		**16**	**ак. ч**
		2						**з.е.**
		54	**13,5**		**28,5**		**12**	**ас.ч.**

Таблица 4.

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущ. контроля успеваемости[2], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам				СР	
			л	лр	пз	**КСР**		
Очно-заочная форма обучения								
Раздел 1	**Основы информационной безопасности**	**28**	**4**		**4**		**20**	
Тема1.1.	Введение в информационную							О
Тема 1.2.	Анализ рисков и оборонительные модели							О ПЗ
Тема 1.3.	Политика безопасности							О ПЗ
Тема 1.4.	Аутентификация и авторизация							О ПЗ

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

Тема 1.5.	Архитектура безопасности							О ПЗ
Раздел 2	**Разработка системы информационной безопасности**	**44**	**4**		**6**		**34**	
Тема 2.1	Межсетевые экраны							О ПЗ
Тема 2.2.	Системы обнаружения атак							О ПЗ
Тема 2.3.	Атака и методы хакеров							О ПЗ
Тема 2.4.	Частные виртуальные сети							О ПЗ
Тема 2.5.	Безопасность беспроводных сетей							О
Промежуточная аттестация								Зачет
Всего:		**72**	**8**		**10**		**54**	**ак. ч**
		2						**з.е.**
		54	**6**		**7,5**		**40,5**	**ас.ч.**

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**		
Заочная форма обучения								
Раздел 1	**Основы информационной безопасности**	**24**	**2**		**2**		**20**	
Тема1.1.	Введение в информационную безопасность системы							О
Тема 1.2.	Анализ рисков и оборонительные модели организации							О ПЗ
Тема 1.3.	Политика безопасности							О ПЗ
Тема 1.4.	Аутентификация и авторизация							О ПЗ

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

Тема 1.5.	Архитектура безопасности							О ПЗ
Раздел 2	**Разработка системы информационной безопасности**	**44**	**2**		**2**		**40**	
Тема 2.1	Межсетевые экраны							О ПЗ
Тема 2.2.	Системы обнаружения атак							О ПЗ
Тема 2.3.	Атака и методы хакеров							О ПЗ
Тема 2.4.	Частные виртуальные сети							О ПЗ
Тема 2.5.	Безопасность беспроводных сетей							О
Промежуточная аттестация		4				4		Зачет
Всего:		**72**	**4**		**4**	**4**	**60**	**ак. ч**
		2						**з.е.**
		54	**3**		**3**	**3**	**45**	**ас.ч.**

Таблица 6.

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущ. контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			л/эо, дот[5]	лр/э, дот	пз/э, дот	**КСР**		
Заочная форма обучения с применением ЭО, ДОТ								
Раздел 1	**Основы информационной безопасности**	**24**	**2**		**2**		**20**	
Тема 1.1.	Введение в информационную безопасность							Электронный семинар
Тема 1.2.	Анализ рисков и оборонительные модели							
Тема 1.3.	Политика безопасности							
Тема 1.4.	Аутентификация и авторизация							

4 Формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), практические задания (ПЗ), электронный семинар (ЭС), письменное контрольное задание (ПКЗ)

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

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							
Выполнение ПКЗ								ПКЗ
Промежуточная аттестация						4		Зачет
Всего:		*72*	**4**		**4**	**4**	**60**	ак. ч
		2						**з.е.**
		54	**3**		**3**	**3**	**45**	**ас.ч.**

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.

Методы текущего контроля успеваемости по очной, очно-заочной и заочной формам обучения

Тема (раздел)		Методы текущего контроля успеваемости
Раздел 1	**Основы информационной безопасности**	
Тема1.1.	Введение в информационную безопасность системы управления	Устный / письменный 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

Таблица 8.

Методы текущего контроля успеваемости по заочной форм обучения с применением ЭО, ДОТ

Тема (раздел)		Методы текущего контроля успеваемости
Раздел 1	**Основы информационной безопасности**	
Тема1.1.	Введение в информационную безопасность системы управления	Письменный ответ на вопрос электронного семинара Письменное собеседование с обучающимся в рамках электронного семинара
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 информационно-аналитических систем**	
Тема 2.1	Межсетевые экраны	Письменный ответ на вопрос электронного семинара Письменное собеседование с обучающимся в рамках электронного семинара
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	

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, информировав 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 оценочные средства по теме 1.1. Введение в информационную безопасность системы управления

Вопросы для опроса

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

Типовые оценочные средства по теме 1.2. Анализ рисков и оборонительные модели организации

Вопросы для опроса

1. Понятие рисков.
2. Что такое векторы угроз?

3. Какие существуют модели защиты?
4. Периметровая защита.

Типовые практические задания

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

Типовые оценочные средства по теме 1.3. Политика безопасности

Вопросы для опроса

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

Типовые практические задания

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

Типовые оценочные средства по теме 1.4. Аутентификация и авторизация

Вопросы для опроса

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

Типовые оценочные средства по теме 1.5 Аутентификация и авторизация

Вопросы для опроса

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

Типовые практические задания

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

Вопросы к электронному семинару по разделу 1

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

Типовые оценочные средства по теме 2.1. Межсетевые экраны

Вопросы для опроса

1. Классификация МЭ.

Типовые практические задания

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

Типовые оценочные средства по теме 2.2. Системы обнаружения атак

Вопросы для опроса

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

Типовые практические задания

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

Типовые оценочные средства по теме 2.3. Атака и методы хакеров

Вопросы для опроса

1. Атаки доступа.
2. Атаки модификации.
3. Переполнение буфера.
4. Распределенные атаки.

Типовые практические задания

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

Типовые оценочные средства по теме 2.4. Частные виртуальные сети

Вопросы для опроса

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

Типовые практические задания

1. Создайте частную виртуальную сеть.

Типовые оценочные средства по теме 2.5. Безопасность беспроводных сетей

Вопросы для опроса

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

Типовые практические задания

1. Создайте частную виртуальную сеть.

Вопросы к электронному семинару по 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 9.

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 на очной, очно-заочной, заочной, формам обучения ПК – 26.2 на заочной с применением ЭО, ДОТ форме обучения	Способность осознавать сущность и значимость информации в современном обществе Способность к информатизации деятельности соответствующих органов власти и организаций

Таблица 10.

Этап освоения компетенции	**Показатель оценивания**	**Критерий оценивания**
ПК-26.3 на очной, очно-заочной, формам обучения 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.

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ПК – 26.2 на заочной с применением ЭО, ДОТ форме обучения Способность к информатизации деятельности соответствующих органов власти и организаций	Знает технические и программные средства реализации информационных процессов. Имеет понятия о локальных и глобальных сетях ЭВМ. Может ориентироваться в основных информационных процессах.	Взаимодействует с главным компонентом АИС - системой управления базами данных (СУБД). Использует информационные системы и средства вычислительной техники в решении задач сбора, передачи, хранения и обработки экономической информации. Использует методы решения экономических задач с помощью АИС.

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 11.

Очная, очно-заочная, заочная форма и заочная форма с применением ЭО, 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..
Зачтено (51-100)	Свободно ориентируется в вопросах обеспечения информационной безопасности при информатизации деятельности организации. Этапы компетенции, предусмотренные образовательной программой, сформированы на высоком уровне. 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.

4.4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Зачет включает ответы на теоретические вопросы и выполнение практических заданий.

Ответы на теоретические вопросы могу 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.

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

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 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 иди иному положению ответа.

Если отвечающий не в состоянии понять и поправить ошибку, преподаватель вызывает другого студента для ее исправления. В необходимых случаях целесообразно наводящими 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.

При применении дистанционной технологии обучения по очной, очно-заочной, заочной (традиционной) форм обучения учебный материал[6], который необходимо

[6] 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.

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.

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. – 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.
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. - 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, 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.

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. — Загл. с экрана. - То же [Электронный ресурс]. — Доступ из ЭБС «IPRbooks». — Режим доступа : http://www.iprbookshop.ru/43960, требуется авторизация. — 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. — 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. — 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. – Загл. с экрана.
4. 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. — Загл. с экрана.
5. 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. — Загл. с экрана.
6. 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. — Загл. с экрана.
7. 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.
8. 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.
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. — Загл. с экрана.

6.3 Учебно-методическое обеспечение самостоятельной работы

1. 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.

6.4 Нормативные правовые документы

6.5. 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.

6.6 Иные источники

Не используются

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

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 практического типа (столы аудиторные, стулья, трибуна, доска аудиторная, компьютер с выходом в Интернет, мультимедийный проектор, экран).

Компьютерные классы (компьютеры с подключением к локальной сети института (включая правовые системы) и Интернет, столы аудиторные, стулья, доски аудиторные)

Помещения для самостоятельной работы обучающихся (компьютеры с подключением 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. Справочные правовые системы «Гарант», «Консультант Плюс», «КонсультантПлюс-Регион»).

Библиотека (компьютеры с подключением к локальной сети филиала и Интернет, Wi-Fi, столы аудиторные, стулья).

Видеостудия для вебинаров (оборудованные компьютерами с выходом в Интернет, оснащенные веб-камерами и гарнитурами (наушники+микрофон), столами и стульями).

Кабинеты (оборудованные компьютерами с выходов в Интернет, в том числе оснащенные веб-камерой, гарнитурой, столами, стульями, принтерами).

Используемое программное обеспечение (MS Word, MS Excel, Acrobat Reader, MS Power Point (или иной редактор презентаций); интернет-браузеры Google Chrome, Yandex; программы просмотра видео (MS Media Player, и другие совместимые с ПО); iSpring Free Cam8).