Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
Пермский национальный исследовательский
политехнический университет

Гуманитарный факультет
(наименование факультета)
кафедра менеджмента и маркетинга
(наименование кафедры, ведущей дисциплину)

УТВЕРЖДАЮ
Проректор по учебной работе
д-р техн. наук, проф.
_____ Н. В. Лобов
«__» _____ 2016 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Информационная безопасность в бизнесе»
(*наименование дисциплины по учебному плану*)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Программа прикладного бакалавриата

Направление 38.03.02 «Менеджмент»
(*код и наименование*)

Профиль программы бакалавриата Маркетинг и инновации
Управление человеческими ресурсами
Менеджмент организации
Менеджмент
(*наименование профиля/маг. программы/специализации*)

Квалификация выпускника: бакалавр
(*бакалавр / магистр / специалист*)

Выпускающая кафедра: Менеджмент и маркетинг
(*наименование кафедры*)

Форма обучения: очная

Курс: _4__. **Семестр**: _8__

Трудоёмкость:
Кредитов по рабочему учебному плану: __3___ ЗЕ
Часов по рабочему учебному плану: __108_ ч

Виды контроля:
Зачет: **1** Диф.зачёт: Курсовой проект: Курсовая работа: -

Пермь 2016

Учебно-методический комплекс дисциплины Информационная безопасность в бизнесе
(полное наименование дисциплины)

разработан на основании:

- федерального государственного образовательного стандарта высшего образования, утверждённого приказом Министерства образования и науки Российской Федерации «12» января 2016 г. номер приказа «7» по направлению подготовки 38.03.02 Менеджмент (уровень бакалавриата);
- компетентностных моделей выпускника ОПОП по направлению подготовки 38.03.02 «Менеджмент» по профилям подготовки: «Менеджмент», «Маркетинг и инновации», «Управление человеческими ресурсами», «Менеджмент организации», утвержденных «24» июня 2013 г. с изменениями в связи с переходом на ФГОС ВО;
- базовых учебных планов очной формы обучения по направлению подготовки 38.03.02 «Менеджмент» по профилям подготовки: «Менеджмент», «Маркетинг и инновации», «Управление человеческими ресурсами», «Менеджмент организации», утвержденных «28» апреля 2016 г.

Рабочая программа согласована с рабочими программами Информационные технологии в менеджменте, Информационные технологии в кадровой работе, Информационные технологии в управлении персоналом, Web технологии в менеджменте, участвующие в формировании компетенций совместно с данной дисциплиной.

Разработчик канд. экон. наук, доцент С.Г. Ахметова

Рецензент канд.экон.наук, проф. Л.В. Невская

Рабочая программа рассмотрена и одобрена на заседании кафедры «Менеджмент и маркетинг» «21 » сентября 2016 г., протокол № 2.

Заведующий кафедрой,
ведущей дисциплину
д-р экон. наук, проф. А.В.Молодчик

Рабочая программа одобрена учебно-методической комиссией Гуманитарного факультета «26» сентября 2016 г., протокол № 3.

Председатель учебно-методической комиссии
д-р соц. наук, проф. В.Н. Стегний

СОГЛАСОВАНО
Начальник управления образовательных
программ, канд. техн. наук, доц. Д. С. Репецкий

1. Общие положения

1.1. Цели дисциплины:

- Приобретение умений и навыков по выявлению угроз и уязвимостей коммерческой информации.
- Формирование у студентов совокупности знаний и навыков по обеспечению защиты коммерческой информации.
- Формирование у студентов совокупности знаний и навыков по обеспечению защиты персональных даных сотрудников.
- Формирование у студентов совокупности знаний и навыков по организации документооборота коммерческой информации.

В процессе изучения данной дисциплины студент расширяет и углубляет следующие компетенции:

- Понимание роли и значения информации и информационных технологий в развитии современного общества и экономических знаний (ОК-16)
- Владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-17).

1.2. Задачи дисциплины:

- получить представление об основных угрозах информационной безопасности предприятия и их источниках;
- научиться использовать необходимые действия для уменьшения рисков и угроз информационной безопасности в коммерческой деятельности;
- получить представление о способах и средствах защиты персональных данных сотрудников
- изучить особенности конфиденциального делопроизводства коммерческой информации;

1.3. Предметом освоения дисциплины являются следующие объекты:

- Система информационной безопасности коммерческой деятельности предприятия.
- Конфиденциальное делопроизводство коммерческой информации.
- Защита персональных данных сотрудников предприятия.

1.4. Место дисциплины в структуре профессиональной подготовки выпускников.

Дисциплина относится к вариативной части ~~профессионального~~ Блок 1 цикла и является дисциплиной по выбору студента.

В результате освоения дисциплины обучающийся должен освоить части указанных в пункте 1.1. компетенций и демонстрировать следующие результаты:

Знать:

- Основные угрозы информационной безопасности коммерческой деятельности предприятия и их источники
- Особенности и задачи конфиденциального делопроизводства, отражающей коммерческую информацию.
- Требования по обеспечению защиты коммерческой информации и информационных систем.
- Требования по обеспечению защиты персональных данных сотрудников
- Современные технологии для защиты конфиденциальной информации предприятия.
- Современные технологии для организации кадрового делопроизводства и защиты персональных данных сотрудников.

Уметь:

- Использовать необходимые действия для уменьшения рисков и угроз информационной безопасности коммерческой деятельности.
- Организовать конфиденциальное делопроизводство, отражающее коммерческую деятельность.
- Организовать защиту коммерческой информации и информационных систем.
- Организовать защиту персональных данных сотрудников.

Владеть:

- Способами выявления угроз и уязвимостей информационной безопасности коммерческой деятельности
- Навыками использования технологий для защиты конфиденциальной коммерческой информации предприятия.
- Навыками использования технологий для организации делопроизводства отражающего коммерческую деятельность. и защиты персональных данных сотрудников.

В таблице 1.1. приведены предшествующие и последующие дисциплины, направленные на формирование компетенций, заявленных в пункте 1.1.

Таблица 1.1. – Дисциплины, направленные на формирование компетенций

Индекс	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Профессиональные компетенции			
ОК-16	Понимание роли и значения информации и информационных технологий в развитии современного общества и экономических знаний	1.Информационные технологии в менеджменте 2. Информационные технологии в управлении персоналом 3.Безопасность жизнедеятельности	
ОК-17	Владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией	1. Информационные технологии в менеджменте 2.Web-технологии в менеджменте	

2. Требования к результатам освоения дисциплины

Учебная дисциплина обеспечивает формирование части компетенций ОК-16 и ОК-17.

2.1.Дисциплинарная карта компетенции

Код	Формулировка компетенции
ОК-16	Понимание роли и значения информации и информационных технологий в развитии современного общества и экономических знаний

Код	Формулировка дисциплинарной части компетенции
ОК-16 Б3.ДВ4.1	Способность выявления угроз экономической безопасности, реализуемой через персонал. Знание работы с персоналом, допущенным к конфиденциальной коммерческой информации

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компонентов студент		
Знает: ▪ Понятие коммерческой тайны ▪ Понятие конфиденциальных коммерческих документов ▪ Понятие угроз экономической безопасности. ▪ Методы работы с информационными ресурсами. ▪ Методы работы по выявлению угроз безопасности коммерческой деятельности ▪ Методы работы по защите информационных ресурсов.	Лекции Презентация	Электронное тестирование Обсуждение в форуме
Умеет: ▪ Различать классы информационных ресурсов предприятия с т.зр. конфиденциальности коммерческой информации ▪ Выявлять угрозы информационной безопасности коммерческой деятельности. ▪ Определять меры по обеспечению защиты информации.	Лекции Практические занятия	Контрольные задания
Владеет ▪ Методами работы с информационными ресурсами предприятия ▪ Методами работы по выявлению угроз безопасности коммерческой деятельности ▪ Методами работы с персональными данными сотрудников	Самостоятельная работа студентов	Контрольная работа (эссе) - защита

2.2. Дисциплинарная карта компетенции

Код	Формулировка компетенции
ОК-17	Владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией

Код	Формулировка дисциплинарной части компетенции
Б3.ДВ4.1	Способность понимать особенности документооборота на цифровых носителях. Знать меры защиты при работе с электронной почтой и ресурсами Интернета.

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
Знает ▪ Особенности конфиденциального документооборота на цифровых носителях. ▪ Меры защиты конфиденциальных документов на цифровых носителях. ▪ Порядок организации архива для хранения конфиденциальных документов на цифровых носителях.	Лекции Презентация	Тестирование Обсуждение в форуме
Умеет ▪ Определять сведения, относимые к коммерческой тайне. ▪ Определять угрозы и уязвимости конфиденциальных документов на цифровых носителях. ▪ Распределять информацию по классам конфиденциальности. ▪ Определять меры к защите конфиденциальных документов на цифровых носителях.	Лекции Практические занятия	Тестирование Контрольные задания
Владеет ▪ Навыками работы с конфиденциальными документами на цифровых носителях. ▪ Навыками работы с определением степени угроз и уязвимостей со стороны Интернета. ▪ Навыками организации архива конфиденциальных документов на цифровых носителях.	Лекции Практические занятия	Подготовка реферата

Таблица 1.1а – Дисциплины, направленные на формирование компетенций

Код	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Общепрофессиональные компетенции			
ОПК-7	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Информационные технологии в менеджменте Информационные технологии в управлении персоналом Информационная безопасность в кадровой работе Веб-технологии в менеджменте	

2.1. Дисциплинарная карта компетенции ОПК-7

Код	Формулировка компетенции:
ОПК-7	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Код	Формулировка дисциплинарной части компетенции:
ОПК-7 **Б2.ДВ1**	Способность выявления угроз экономической безопасности, реализуемой через персонал. Знание этапов работы по выявлению угроз и уязвимостей коммерческой информации

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
Знает ▪ Основные угрозы информационной безопасности коммерческой информации предприятия и их источники ▪ Понятие конфиденциальные документы ▪ Требования по обеспечению защиты персональных данных сотрудников ▪ Современные технологии для защиты персональных данных сотрудников ▪ Современные технологии для защиты конфиденциальной информации предприятия.	Лекция Презентация Видеоуроки	Тестирование Обсуждение в форуме
Умеет ▪ Различать классы информационных ресурсов предприятия с т.зр. конфиденциальности ▪ Определять меры по обеспечению защи-	Практические занятия	Контрольные задания

ты информации. ▪ Определять меры по обеспечению защиты персональных данных сотрудников		
Владеет ▪ Методами работы с информационными ресурсами предприятия и выявления угроз, уязвимостей коммерческой информации ▪ Методами работы по обеспечению защиты персональных данных сотрудников ▪ Методами работы по организации делопроизводства	Практические занятия	Контрольная работа

3 Структура учебной дисциплины по видам и формам учебной работы

Таблица 3.1 – Объём и виды учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость		
		по семестрам		всего
1	**Аудиторная работа / в том числе в интерактивной форме**	-	50 / 10	50
	Лекции (Л) / в том числе в интерактивной форме	-	14 / 4	14
	Практические занятия (ПЗ) / в том числе в интерактивной форме	-	36 / 6	36
	Лабораторные работы (ЛР)	-	-	-
2	Контроль самостоятельной работы (КСР)	-	4	4
3	**Самостоятельная работа студентов** (СРС)	-	98	98
	Изучение теоретического материала	-	48	48
	Расчётно-графические работы	-	-	-
	Подготовка к индивидуальным и групповым заданиям на практических занятиях по: - определению угроз и уязвимостей коммерческой информации. - определению рисков компьютерной информационной системы. -организации конфиденциального документооборота. - определению способов защиты от неправомерных действий сотрудников. - определению способов защиты цифровых документов и контроля использования ресурсов Интернета.		50	50
	Другие виды самостоятельной работы: самостоятельная работа студентов по решению практических задач	-	-	-
4	Итоговая аттестация по дисциплине: *зачёт / экзамен*	-	дифференцированный зачет	
5	**Трудоёмкость дисциплины** **Всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	-	**152 ч.** **4 ЗЕ**	**152 ч.** **4 ЗЕ**

Таблица 3.1 – Объём и виды учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость		
		по семестрам		всего
1	**Аудиторная работа / в том числе в интерактивной форме**	-	41	41
	Лекции (Л) / в том числе в интерактивной форме	-	14	14
	Практические занятия (ПЗ) / в том числе в интерактивной форме	-	27	27
	Лабораторные работы (ЛР)	-	-	-
2	Контроль самостоятельной работы (КСР)	-	4	4
3	**Самостоятельная работа студентов** (СРС)	-	63	63
	Изучение теоретического материала	-	33	33
	Расчётно-графические работы	-	-	-
	Подготовка к индивидуальным и групповым заданиям на практических занятиях по: - определению угроз и уязвимостей коммерческой информации. - определению рисков компьютерной информационной системы. -организации конфиденциального документооборота. - определению способов защиты от неправомерных действий сотрудников. - определению способов защиты цифровых документов и контроля использования ресурсов Интернета.		30	30
	Другие виды самостоятельной работы: самостоятельная работа студентов по решению практических задач	-	-	-
4	Итоговая аттестация по дисциплине: *зачёт / экзамен*	-	зачет	
5	**Трудоёмкость дисциплины** **Всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	-	**108 ч.** **3 ЗЕ**	**108 ч.** **3 ЗЕ**

4. Содержание учебной дисциплины

4.1. Модульный тематический план

Таблица 4.1 – Тематический план по модулям учебной дисциплины

Номер учебного модуля	Номер раздела дисциплины	Номер темы дисциплины	Количество часов (очная форма обучения)							Трудоёмкость, ч / ЗЕ
			аудиторная работа					Итог аттест	самостоятельная работа	
			всего	Л	ПЗ	ЛР	КСР			
1	2	3	4	5	6	7	8	9	10	11
1	1	1	6	2	4					
		2	5	1	4	-		-		
		3	6	2	4					
		4	5	1	4					
		5	6	2	4					
	Итого по модулю:		**28**	**8**	**20**	**-**	**2**		**48**	**98**
2	2	6	8	2	6	-				
		7	8	2	6					
		8	6	2	4					
	Итого по модулю:		**22**	**6**	**9**	**-**	**2**		**50**	**50**
Итоговая аттестация						-		**Диф. зачет**		
Всего:			**50**	**14**	**36**	**-**	**4**		**98**	**152**

Таблица 4.1 – Тематический план по модулям учебной дисциплины

Номер учебного модуля	Номер раздела дисциплины	Номер темы дисциплины	Количество часов (очная форма обучения)							Трудоёмкость, ч / ЗЕ
			аудиторная работа					Итог аттест	самостоятельная работа	
			всего	Л	ПЗ	ЛР	КСР			
1	2	3	4	5	6	7	8	9	10	11
1	1	1	6	2	2					
		2	5	1	4	-		-		
		3	6	2	4					
		4	5	1	4					
		5	6	2	4					
	Итого по модулю:		**26**	**8**	**18**	**-**	**2**		**33**	**61**
2	2	6	8	2	3	-				
		7	8	2	3					
		8	6	2	3					
	Итого по модулю:		**15**	**6**	**9**	**-**	**2**		**30**	**47**
Итоговая аттестация						-		**Диф. зачет**		
Всего:			**41**	**14**	**27**	**-**	**4**		**63**	**108**

4.2. Содержание разделов и тем учебной дисциплины

Модуль 1. Концепция информационной безопасности

Раздел 1. Концепция информационной безопасности

Л – 8 ч, ПЗ – 20 ч, ЛР - нет, СРС –48

Тема 1. Информационные ресурсы и конфиденциальность информации

Классификация информации с точки зрения информационной безопасности. Интеллектуальная собственность, патент, авторское право, коммерческая тайна. Защита коммерческой тайны. Порядок разработки перечня конфиденциальной коммерческой информации

Федеральный закон «Об информации, информатизации и защите информации».

Тема 2. Угрозы конфиденциальной информации и системы ее защиты

Риски угроз информационной безопасности, связанные с коммерческой деятельностью компании. Внешние и внутренние источники угроз. Несанкционированное уничтожение документов, подмена или изъятие документов, фальсификация текста или его части. Каналы несанкционированного доступа. Составляющие системы защиты. Организационно-правовая система защиты.

Тема 3. Конфиденциальное делопроизводство

Особенности и задачи конфиденциального делопроизводства. Организация конфиденциального делопроизводства. Подготовка и издание конфиденциальных документов. Разрешительная система доступа к конфиденциальным документам. Формирование и оформление конфиденциальных дел. Проверка наличия конфиденциальных документов.

Тема 4. Персонал, владеющий конфиденциальной информацией

Формы угроз экономической безопасности фирмы, реализуемые через ее персонал. Этапы работы с сотрудниками, допущенными к конфиденциальной информации. Этап приема сотрудника, этап непосредственной деятельности, этап увольнения сотрудника, имеющего допуск к конфиденциальной информации.

Тема 5. Конфиденциальный документооборот

Принципы организации конфиденциального документооборота. Разрешительная система допуска сотрудников к конфиденциальным документам. Персональная и обязательная ответственности за выдачу неправомерных разрешений на ознакомление с конфиденциальными документами и на их отправление.

Модуль 2. Информационная безопасность коммерческой деятельности

Раздел 2. Информационная безопасность коммерческой деятельности

Л – 6 ч, ПЗ – 16 ч, ЛР - нет, КСР – 4 ч., СРС – 50 ч.

Тема 6. Конфиденциальный документооборот на цифровых носителях

Особенности документооборота на цифровых носителях. Меры защиты в отношении цифровых документов. Программно-аппаратный контроль. Организационно-технический контроль. Процедуры контроля использования мобильных носителей информации. Процедуры контроля использования ресурсов Интернета. Требования к организации электронного архива конфиденциальных документов.

Тема 7. Обеспечение информационной безопасности коммерческой деятельности

Выявление перечня потенциально возможных угроз интересам предприятия. Наиболее распространенные угрозы: угрозы несанкционированного доступа; программные вирусы; угрозы отказа оборудования; угрозы сбоев программного обеспечения. Определение возможного ущерба, который может возникнуть в результате реализации подобных угроз.

Тема 8. Стандарты информационной безопасности

Функции стандартов: выработка понятийного аппарата и терминологии в области информационной безопасности; формирование шкалы измерений уровня информационной безопасности; накопление сведений о лучших практиках обеспечения информационной безопасности. Британский стандарт BS 7799. Аудит системы управления информационной безопасности. Политика информационной безопасности.

4.2. Содержание разделов и тем учебной дисциплины

Модуль 1. Концепция информационной безопасности

Раздел 1. Концепция информационной безопасности

Л – 8 ч, ПЗ – 18 ч, КСР - 2, СРС –33

Тема 1. Информационные ресурсы и конфиденциальность информации

Классификация информации с точки зрения информационной безопасности. Интеллектуальная собственность, патент, авторское право, коммерческая тайна. Защита коммерческой тайны. Порядок разработки перечня конфиденциальной коммерческой информации

Федеральный закон «Об информации, информатизации и защите информации».

Тема 2. Угрозы конфиденциальной информации и системы ее защиты

Риски угроз информационной безопасности, связанные с коммерческой деятельностью компании. Внешние и внутренние источники угроз. Несанкционированное уничтожение документов, подмена или изъятие документов, фальсификация текста или его части. Каналы несанкционированного доступа. Составляющие системы защиты. Организационно-правовая система защиты.

Тема 3. Конфиденциальное делопроизводство

Особенности и задачи конфиденциального делопроизводства. Организация конфиденциального делопроизводства. Подготовка и издание конфиденциальных документов. Разрешительная система доступа к конфиденциальным документам. Формирование и оформление конфиденциальных дел. Проверка наличия конфиденциальных документов.

Тема 4. Персонал, владеющий конфиденциальной информацией

Формы угроз экономической безопасности фирмы, реализуемые через ее персонал. Этапы работы с сотрудниками, допущенными к конфиденциальной информации. Этап приема сотрудника, этап непосредственной деятельности, этап увольнения сотрудника, имеющего допуск к конфиденциальной информации.

Тема 5. Конфиденциальный документооборот

Принципы организации конфиденциального документооборота. Разрешительная система допуска сотрудников к конфиденциальным документам. Персональная и обязательная ответственности за выдачу неправомерных разрешений на ознакомление с конфиденциальными документами и на их отправление.

Модуль 2. Информационная безопасность коммерческой деятельности

Раздел 2. Информационная безопасность коммерческой деятельности

Л – 6 ч, ПЗ – 9 ч, ЛР - нет, КСР – 2 ч., СРС – 30 ч.

Тема 6. Конфиденциальный документооборот на цифровых носителях

Особенности документооборота на цифровых носителях. Меры защиты в отношении цифровых документов. Программно-аппаратный контроль. Организационно-технический контроль. Процедуры контроля использования мобильных носителей информации. Процедуры контроля использования ресурсов Интернета. Требования к организации электронного архива конфиденциальных документов.

Тема 7. Обеспечение информационной безопасности коммерческой деятельности

Выявление перечня потенциально возможных угроз интересам предприятия. Наиболее распространенные угрозы: угрозы несанкционированного доступа; программные вирусы; угрозы отказа оборудования; угрозы сбоев программного обеспечения. Определение возможного ущерба, который может возникнуть в результате реализации подобных угроз.

Тема 8. Стандарты информационной безопасности

Функции стандартов: выработка понятийного аппарата и терминологии в области информационной безопасности; формирование шкалы измерений уровня информационной безопасности; накопление сведений о лучших практиках обеспечения информационной безопасности. Британский стандарт BS 7799. Аудит системы управления информационной безопасности. Политика информационной безопасности.

4.3. Перечень тем практических занятий

Таблица 4.2 – Темы практических занятий

№ п.п.	Номер темы дисциплины	Наименование темы практического занятия
1	1	Определение сведений, относимых к коммерческой тайне. Составление перечня документов по классам конфиденциальности. Выполнение задания.
2	2	Выявление угроз и уязвимостей информационной безопасности. Определение мер для снижения рисков угроз информационной безопасности. Выполнение задания.
3	3	Составление перечня конфиденциальных документов. Разработка разрешительной системы допуска к конфиденциальным документам. Выполнение задания.
4	4	Выявление угроз безопасности, реализуемые через персонал. Разработка процедур работы с конфиденциальными документами. Выполнение задания.
5	5	Угрозы и уязвимости конфиденциального документооборота на цифровых носителях. Разрешительная система допуска сотрудников к конфиденциальным документам. Выполнение задания.
6	6	Документооборот на цифровых носителях. Меры защиты в отношении цифровых документов. Групповая работа над проектом.
7	7	Определение перечня потенциально возможных угроз интересам предприятия. Определение возможного ущерба, который может возникнуть в результате реализации подобных угроз. Групповая работа над проектом
8	8	Проведение аудита системы управления информационной безопасности. Политика информационной безопасности.

4.5. Виды самостоятельной работы студентов

Таблица 4.3 – Виды самостоятельной работы студентов (СРС)

Номер темы дисциплины	Вид самостоятельной работы студентов	Трудоёмкость, часов
1	*Изучение теоретического материала:* - Интеллектуальная собственность, патент, авторское право, коммерческая тайна. Защита коммерческой тайны. Порядок разработки перечня конфиденциальной информации Федеральный закон «Об информации, информатизации и защите информации». *подготовка к тестированию*	8
2	*Изучение теоретического материала:* - Правовая, организационная, инженерно-техническая, программно-аппаратная и криптографическая составляющие системы защиты цифровой информации *подготовка к тестированию*	8
3	*Подготовка к практическим занятиям:* - Определение угроз и уязвимостей коммерческой информации. - Риски информационной безопасности. Основные подходы к управлению рисками. - Определение рисков компьютерной информационной системы.	12
4	*Изучение теоретического материала:* - Сущность и особенности конфиденциального документооборота. Особенности и задачи конфиденциального делопроизводства. - Организация конфиденциального делопроизводства. Подготовка и издание конфиденциальных документов. - Организация конфиденциального документооборота. Формирование и оформление конфиденциальных дел	12
5	*Подготовка к практическим занятиям:* - Персонал, владеющий конфиденциальной информацией. Непреднамеренные ошибки пользователей. Обиженные сотрудники. Несанкционированный доступ к конфиденциальной информации. Системы защиты от неправомерных действий сотрудников.	12
6	*Изучение теоретического материала:* Особенности документооборота на цифровых носителях. Меры защиты в отношении цифровых документов. Процедуры контроля использования мобильных носителей информации. Процедуры контроля использования ресурсов Интернета	12
7	*Подготовка к практическим занятиям:*	18

	Определение перечня потенциально возможных угроз интересам предприятия. Определение возможного ущерба, который может возникнуть в результате реализации подобных угроз	
8	*Подготовка к практическим занятиям:* Аудит системы управления информационной безопасности. Политика информационной безопасности.	16
	Итого: в **ч** / в **ЗЕ**	98

Таблица 4.3 – Виды самостоятельной работы студентов (СРС)

Номер темы дисциплины	**Вид самостоятельной работы студентов**	**Трудоёмкость, часов**
1	*Изучение теоретического материала:* - Интеллектуальная собственность, патент, авторское право, коммерческая тайна. Защита коммерческой тайны. Порядок разработки перечня конфиденциальной информации Федеральный закон «Об информации, информатизации и защите информации». *подготовка к тестированию*	8
2	*Изучение теоретического материала:* - Правовая, организационная, инженерно-техническая, программно-аппаратная и криптографическая составляющие системы защиты цифровой информации *подготовка к тестированию*	8
3	*Подготовка к практическим занятиям:* - Определение угроз и уязвимостей коммерческой информации. - Риски информационной безопасности. Основные подходы к управлению рисками. - Определение рисков компьютерной информационной системы.	8
4	*Изучение теоретического материала:* - Сущность и особенности конфиденциального документооборота. Особенности и задачи конфиденциального делопроизводства. - Организация конфиденциального делопроизводства. Подготовка и издание конфиденциальных документов. - Организация конфиденциального документооборота. Формирование и оформление конфиденциальных дел	8
5	*Подготовка к практическим занятиям:* - Персонал, владеющий конфиденциальной информацией. Непреднамеренные ошибки пользователей. Обиженные сотрудники. Несанкционированный доступ к конфиденциаль-	8

	ной информации. Системы защиты от неправомерных действий сотрудников.	
6	*Изучение теоретического материала:* Особенности документооборота на цифровых носителях. Меры защиты в отношении цифровых документов. Процедуры контроля использования мобильных носителей информации. Процедуры контроля использования ресурсов Интернета	8
7	*Подготовка к практическим занятиям:* Определение перечня потенциально возможных угроз интересам предприятия. Определение возможного ущерба, который может возникнуть в результате реализации подобных угроз	8
8	*Подготовка к практическим занятиям:* Аудит системы управления информационной безопасности. Политика информационной безопасности.	7
	Итого: в **ч** / в **ЗЕ**	6

5. Образовательные технологии, используемые для формирования компетенций

Лекционные занятия проводятся с использованием презентаций и демонстрации соответствующих программ. В процессе лекций постоянно проводится опрос по ранее пройденному материалу. Материалы лекций опубликованы на странице дисциплины на портале гуманитарного факультета[1].

Практические занятия проводятся в учебной аудитории. Все контрольные задания, тесты и дополнительный материал также опубликованы на портале на странице дисциплины. При проведении практических занятий преследуются следующие цели:

- освоение работы с конфиденциальными документами, содержащими коммерческую информацию;
- закрепление навыков выявления угроз и уязвимостей информационных систем, связанных с действиями персонала.
- отработка навыков для определения мер по защите информационных систем.
- отработка навыков для определения мер по защите коммерческой инфомации.

Место преподавателя в интерактивных занятиях сводится к направлению деятельности учащихся на достижение целей занятия.

6. Фонд оценочных средств дисциплины

6.1. Текущий и промежуточный контроль освоения заданных дисциплинарных частей-компетенций

Текущий и промежуточный контроль освоения заданных дисциплинарных частей компетенций проводится в форме рейтинговой оценки всех практических занятий, теоретических опросов на лекциях.

[1] URL http://portal-hsb.pstu.ru

6.2. Рубежный контроль освоения заданных дисциплинарных частей компетенций

Рубежный контроль освоения заданных дисциплинарных частей компетенций проводится по окончании модулей дисциплины в следующих формах:

- *тестирование (тема 1-3);*
- *оценка выполненных заданий (темы 3-8).*

6.3. Итоговый контроль освоения заданных дисциплинарных частей компетенций

1) Зачёт по результатам выполненных контрольных заданий и тестирования.

К зачету по дисциплине допускаются студенты, успешно освоившие теоретический материал по итогам проведённого промежуточного контроля и выполнившие все контрольные задания.

Фонды оценочных средств, включающие контрольные задания, тесты и методы оценки, критерии оценивания, перечень контрольных точек и таблица планирования результатов обучения, позволяющие оценить результаты освоения данной дисциплины, входят в состав УМКД в виде приложения.

6.4. Виды текущего, рубежного и итогового контроля освоения элементов и частей компетенций

Таблица 6.4 - Виды контроля освоения элементов и частей компетенций

Контролируемые результаты освоения дисциплины (ЗУВы)	**Вид контроля**					
	ТТ	**РТ**	**КР**	**КР (ГР)**	**Трен. (ЛР)**	**Экзамен**
В результате освоения дисциплины студент:						
Знает:				Не предусмотрены		Не предусмотрен
- Понятие коммерческой тайны. - Понятие конфиденциальных коммерческих документов. - Понятие угроз экономической безопасности. - Методы работы с информационными ресурсами. - Методы работы по выявлению угроз безопасности коммерческой деятельности - Методы работы по защите информационных ресурсов.	+	+		-		
Умеет:						
- Различать классы информационных ресурсов предприятия с т.зр. конфиденциальности коммерческой информации - Выявлять угрозы информационной безопасности коммерческой деятельности.				-	+	

- Определять меры по обеспечению защиты коммерческой информации.						
Владеет:						
- Методами работы с информационными ресурсами предприятия. - Методами работы по выявлению угроз безопасности коммерческой деятельности. - Методами работы с персональными данными сотрудников.	-	-	+	-	+	-

ТТ – текущее тестирование (контроль знаний по теме);

РТ – рубежное тестирование по модулю (автоматизированная система контроля знаний);

КР – рубежная контрольная работа по модулю (оценка умений);

ГР (КР) – индивидуальные графические или курсовые работы (оценка умений и владений);

Трен. (ЛР) – выполнение контрольных заданий с подготовкой отчёта (оценка владения).

7 График учебного процесса по дисциплине

Таблица 7.1 – График учебного процесса по дисциплине

Вид работы	**Распределение часов по учебным неделям**																	**Итого**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	
Раздел:	**Р1**									**Р2**									
Лекции	**2**		**2**		**2**		**2**	**-**		**2**		**2**		**1**		**1**			**14**
Практические занятия	2	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**36**
Семинары																			
Лабораторные работы																			**-**
КСР					**2**												**2**		**4**
Изучение теоретического материала	**-**	**2**	**2**	**4**	**2**	**2**	**2**	**4**	**2**	**2**	**2**	**2**	**2**	**2**	**4**	**2**	**2**	**2**	**40**
Подготовка к занятиям	**-**	**4**	**2**	**4**	**2**	**4**	**4**	**2**	**4**	**2**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**2**	**58**
	4	**8**	**8**	**10**	**10**	**8**	**10**	**8**	**8**	**8**	**8**	**10**	**8**	**9**	**10**	**9**	**10**	**6**	**152**

Модуль:	**М1**									**М2**									
Контр. тестирование					1							1							
Дисциплин. контроль																			**зачёт**

Таблица 7.1 – График учебного процесса по дисциплине

Вид работы	**Распределение часов по учебным неделям**																		**Итого**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	
Раздел:	**Р1**									**Р2**									
Лекции	**2**		**2**		**2**		**2**	**-**		**2**		**2**		**1**		**1**			**14**
Практические занятия	2	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**		**2**		**2**		**2**		**1**	**27**
Семинары																			
Лабораторные работы																			**-**
КСР					**2**												**2**		**4**
Изучение теоретического материала	**-**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**2**	**33**
Подготовка к занятиям	**-**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**1**	**2**	**1**	**1**	**30**
	4	**8**	**8**	**10**	**10**	**8**	**10**	**8**	**8**	**8**	**8**	**10**	**8**	**9**	**10**	**9**	**10**	**6**	**108**
Модуль:	**М1**									**М2**									
Контр. тестирование					1							1							
Дисциплин. контроль																			**зачёт**

8 Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

8.1 Карта обеспеченности дисциплины учебно-методической литературой

Б2.ДВ1 Информационная безопасность в бизнесе	**Блок 1** (*цикл дисциплины*)	
(*полное название дисциплины*)	[ ] основная [X] по выбору студента	[ ] базовая часть цикла [X] вариативная часть цикла

38.03.02	***Менеджмент, профили Менеджмент организации*** ***Управление человеческими ресурсами, Маркетинг и инновации, Менеджмент***
(*код направления / специальности*)	(*полное название направления подготовки / специальности*)

МН/МК, УЧР, МЕН, МО	Уровень подготовки		Форма обучения	
(*аббревиатура направления / специальности*)	[ ]	специалист	[×]	очная
	[×]	бакалавр	[ ]	заочная
	[ ]	магистр	[ ]	очно-заочная

2016 Семестр(ы) 8

Количество групп 2

Количество студентов 40

Ахметова С.Г. доцент

Гуманитарный

Менеджмент и маркетинг 2198300 asg@pstu.ru

8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

№	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1	2	3
1 Основная литература		
1	Информационная безопасность. Учебно-методическое пособие. Ахметова С.Г. Изд-во ПНИПУ, 2013, 122 с.	*5 +ЭБ На кафедре 20*
2	Информационная безопасность. Электронное мультимедийное пособие. Ахметова С.Г. Изд-во ПНИПУ, 2013	CD-ROM
2 Дополнительная литература		
2.1. Учебные и научные издания		
1	Мельников В.П. и др. Защита информации. Учебник для вузов. М. Академия, 2014, 296 с.	6
2	Ахметова С.Г.Информационная безопасность. Электронный курс. http://portal-hsb.pstu.ru	
2.2. Периодические издания		
Не используются		
2.3.Нормативно-технические издания		
	Не используются	
2.4 Официальные данные		
	Не используются	
2.5 Электронные информационно-образовательные ресурсы		
	1. Электронная библиотека Пермского национального исследовательского политехнического университета [Электронный ресурс] : [полнотекстовая база данных электрон. док., издан. в Изд-ве ПНИПУ] / Перм. нац. исслед. политехн. ун-т, Науч. б-ка. – Электрон. текстовые дан. – Пермь, 2014-2015. – Режим доступа: http://elib.pstu.ru, свободный. – Загл. с экрана. 2. Учебно-образовательный портал гуманитарного факультета ПНИПУ – Режим доступа: http://portal-hsb.pstu.ru, ограниченный	

Карта книго-обеспеченности в библиотеку сдана

Основные данные об обеспеченности на ___ 1.12.2013 _____
(*дата составления рабочей программы*)

основная литература	[×]	обеспечена	[ ]	не обеспечена
дополнительная литература	[×]	обеспечена	[ ]	не обеспечена

Зав. отделом комплектования
научной библиотеки _____ Н.В. Тюрикова

Текущие данные об обеспеченности на _____ _____

основная литература	[ ]	обеспечена	[ ]	не обеспечена
дополнительная литература	[ ]	обеспечена	[ ]	не обеспечена

Зав. отделом комплектования
научной библиотеки _____ Н.В. Тюрикова

Карта книго-
обеспеченности
в библиотеку сдана

8.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.3.1. Перечень программного обеспечения, в том числе компьютерные обучающие и контролирующие программы

Таблица 8.1 – Программы, используемые для обучения и контроля

№ п.п.	Вид учебного занятия	Наименование Программного продукта	Рег. номер	Назначение
1	Л	PowerPoint Camtasio Studio		Презентационное сопровождение лекционного материала
3	ПЗ	Учебно-образовательный портал		Электронное тестирование

8.4. Аудио- и видео-пособия

Таблица 8.2 – Используемые аудио- и видео-пособия

Вид аудио-, видео-пособия				Наименование учебного пособия
теле-фильм	кино-фильм	слайды	аудио-пособие	
		+	+	Содержится в электронном курсе «Информационная безопасность»

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

9.1. Специализированные лаборатории и классы

Таблица 9.1 – Специализированные лаборатории и классы

№ п.п.	Помещения			Площадь, $м^2$	Количество посадочных мест
	Название	Принадлежность (кафедра)	Номер аудитории		
1	Лекционная аудитория (мультимедийный класс)	ГУМФ	506 к.А., 516 к.А	80	40

9.2. Основное учебное оборудование

Таблица 9.2 – Учебное оборудование

№ п.п.	Наименование и марка оборудования (стенда, макета, плаката)	Кол-во, ед.	Форма приобретения / владения (собственность, оперативное управление, аренда и т.п.)	Номер аудитории
1	Компьютеры	*30*	*Оперативное управление*	*516 к.А*

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1	2	3
1		
2		
3		
4		

Оценочные средства
для итогового контроля по учебной дисциплине
«Информационная безопасность в бизнесе»

Направление	38.03.02 Менеджмент
Квалификация (степень) выпускника:	Бакалавр
Выпускающая кафедра:	Менеджмент и маркетинг
Вид контроля	Зачет

Список вопросов к зачету

1. Что такое информационная безопасность?
2. Перечислите виды информации с ограниченным доступом.
3. Что относится к информации, интеллектуально ценной для организации?
4. Что такое коммерческая тайна?
5. Перечислите сведения, составляющие коммерческую тайну.
6. Перечислите признаки сведений, составляющих коммерческую тайну.
7. Каковы основные положения Федерального закона «О коммерческой тайне»?
8. Каков порядок разработки перечня конфиденциальной информации в организации?
9. Что включает в себя понятие «Угроза информационной безопасности?
10. Каково соотношение внешних и внутренних угроз информационных ресурсов организации?
11. Перечислите возможные каналы несанкционированного доступа?
12. Перечислите основные виды организационных каналов несанкционированного доступа.
13. Что такое «легальные и нелегальные» методы получения информации?
14. Перечислите методы получения конфиденциальной информации.
15. Перечислите составляющие системы защиты информации.
16. Что включают организационные меры защиты информации?
17. Что включают инженерно-технические элементы защиты информации?
18. Что включают программно-аппаратные средства защиты информации?
19. Перечислите направления аналитической работы в сфере безопасности.
20. Перечислите виды угроз экономической безопасности фирмы.
21. Какие формы могут принимать угрозы безопасности, реализуемые через персонал?
22. Как можно организовать защиту безопасности со стороны персонала организации?
23. Каковы главные определения Федерального закона «О персональных даных»?
24. Перечислите возможные мероприятия по защите персональных данных.
25. Каковы требования по защите предъявляются к каналам передачи персональных данных?
26. Что означают понятия «Конфиденциальные документы» и «Конфиденциальный документооборот»?
27. Какова основная цель защиты конфиденциальной информации?
28. Перечислите формы проявления уязвимостей конфиденциальных документов.
29. Какие меры следует принять для защиты конфиденциальной информации?
30. Перечислите принципы организации конфиденциального документооборота.
31. Что означает «разрешительная система доступа к конфиденциальным документам»?
32. Каковы особенности конфиденциального документооборота на цифровых носителях?

33. Перечислите меры защиты конфиденциальных документов на цифровых носителях.
34. Перечислите правила хранения конфиденциальных документов.
35. Каким образом рекомендуется организовывать архив для хранения конфиденциальных документов.
36. Что такое электронный архив?
37. В чем основные преимущества электронного архива?
38. Перечислите стандартные функции электронного архива.
39. Какие программы для организации электронного архива вам известны?
40. Перечислите компоненты для системного решения задач обеспечения информационной безопасности.
41. Перечислите наиболее распространенные угрозы, которым подвержены информационные системы.
42. Какие угрозы информационной безопасности являются самыми частыми и опасными?
43. Что такое компьютерный вирус и какие из них вам известны?
44. Что такое шпионская программа, какие их разновидности вам известны?
45. Отличаются ли риски информационной безопасности для предприятий разных сфер деятельности?
46. На чем должна основываться стратегия управления рисками?
47. Какими средствами можно воспользоваться для уменьшения риска?
48. Что такое базовый уровень информационной безопасности?
49. Что такое активный аудит системы управления информационной безопасности?
50. Что такое экспертный аудит системы управления информационной безопасности?
51. Из каких разделов должна состоять политика информационной безопасности?

Разработчик
канд.экон. наук, доцент С.Г. Ахметова