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
06 2017 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ

«Информационная безопасность в кадровой работе»

(наименование дисциплины по учебному плану)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программа прикладного бакалавриата

Направление 38.03.03 «Управление персоналом»

(код и наименование)

Профиль программы бакалавриата Управление персоналом организации

(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: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч

Виды контроля:

Диф.зачёт: 2 сем

Пермь 2017

Учебно-методический комплекс дисциплины Информационная безопасность в кадровой работе

(полное наименование дисциплины)

разработан на основании:

- федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерством образования и науки Российской Федерации «14» декабря 2015 г. номер приказа «1461» по направлению подготовки 38.03.03 «Управление персоналом» (уровень бакалавриата);
- компетентностной модели выпускника ОПОП по направлению подготовки 38.03.03 «Управление персоналом» по профилю подготовки: «Управление персоналом организации» «24» июня 2013 г. с изменениями в связи с переходом на ФГОС ВО;
- базового учебного плана очной формы обучения и учебного плана заочной формы обучения по направлению подготовки 38.03.03 «Управление персоналом» по профилю подготовки: «Управление персоналом организации» утвержденных «28» апреля 2016 г.

Рабочая программа согласована с рабочими программами Информационная безопасность в бизнесе, участвующей в формировании компетенций совместно с данной дисциплиной.

Разработчик	канд. экон. наук, доцент		С.Г. Ахметова
Рецензент	докт.экон.наук, проф.		И.А. Эсаулова

Рабочая программа рассмотрена и одобрена на заседании кафедры «Менеджмент и маркетинг» «10 » мая 2017 г., протокол № 17.

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

Рабочая программа одобрена учебно-методической комиссией Гуманитарного факультета «22» мая 2017 г., протокол № 19.

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: Формирование у студентов совокупности знаний и навыков по защите информации, выявлению угроз и уязвимостей, обеспечению защиты персональных данных сотрудников, кадровой информации и информационных систем по обработке кадровой информации.

В процессе изучения данной дисциплины студент осваивает две компетенции:

ОПК-10. Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ПК-27. владение методами и программными средствами обработки деловой информации, навыками работы со специализированными кадровыми компьютерными программами, способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы при решении задач управления персоналом

1.2 Задачи дисциплины:

Формирование знаний

- Изучение основных угроз информационной безопасности кадровой информации, персональных данных сотрудников и их источниках, а также знать классы информационных ресурсов по степени конфиденциальности.

Формирование умений

- использовать необходимые действия для уменьшения рисков и угроз кадровой информации и персональным данным сотрудников.

- уметь оргснизовать защиту персональных данных сотрудников.

Формирование навыков

- владеть способами и средствами защиты информационных ресурсов и персональных данных сотрудников

1.3 Предметом освоения дисциплины являются следующие объекты:

- Система информационной безопасности кадровой информации предприятия
- Конфиденциальное делопроизводство
- Персональные данные сотрудников

1.4 Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность в кадровой работе» относится к вариативной части блока 1 и является обязательной при освоении ОПОП по направлению «Управление персоналом».

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

Код	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Профессиональные компетенции			
ОПК-10	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		
ПК-27	Владением методами и программными средствами обработки деловой информации, навыками работы со специализированными кадровыми компьютерными программами, способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы при решении задач управления персоналом		Информационная безопасность в бизнесе

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

Учебная дисциплина обеспечивает формирование части компетенций ПК-27 и ОПК-10

2.1. Дисциплинарная карта компетенции ПК-27

Код	Формулировка компетенции:
ПК-27	владением методами и программными средствами обработки деловой информации, навыками работы со специализированными кадровыми компьютерными программами, способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы при решении задач управления персоналом

Код	Формулировка дисциплинарной части компетенции:
ПК-27 **Б1.В.02**	Способность выявления угроз экономической безопасности, реализуемой через персонал. Знание этапов работы с персоналом, допущенным к конфиденциальной информацией.

2.2. Дисциплинарная карта компетенции ОПК-10

Код	Формулировка компетенции:
ОПК-10	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-10 **Б1.В.02**	Способность выбирать методы защиты информации и умение обеспечивать защиту информации. Умение работать с персональными данными.

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
Знает ▪ Основные угрозы информационной безопасности кадровой информации предприятия и их источники ▪ Классы информационных ресурсов по степени конфиденциальности	Лекция Презентация Видеоуроки	Теоретический опрос Зачет
Умеет ▪ Использовать необходимые действия для уменьшения рисков и угроз информационной безопасности ▪ Организовать защиту персональных данных сотрудников ▪ Организовать архивное хранение кадровых документов	Практические занятия	Практические занятия
Владеет ▪ Методами работы с информационными ресурсами предприятия и выявления угроз, уязвимостей кадровой информации ▪ Методами работы по обеспечению защиты персональных данных сотрудников ▪ Методами работы по организации кадрового делопроизводства	Практические занятия Самостоятельная работа	Индивидуальные задания

3 Структура учебной дисциплины по видам и формам учебной работы

Объем дисциплины в зачетных единицах составляет 4 ЗЕ. Количество часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся указано в таблице 3.1

Таблица 3.1 – Объём и виды учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость		
			8 семестр	всего
1	**Аудиторная контактная работа / в том числе в интерактивной форме**	-	90/6	90
	Лекции (Л) / в том числе в интерактивной форме	-	14/3	14
	Практические занятия (ПЗ) / в том числе в интерактивной форме	-	72/3	72
	Лабораторные работы (ЛР)	-	-	-
2	Контроль самостоятельной работы (КСР)	-	4	4
3	**Самостоятельная работа студентов** (СРС)	-	54	54
	Изучение теоретического материала	-	14	14
	Расчётно-графические работы	-	-	-
	Индивидуальные задания		20	20
	Подготовка к практическим занятиям	-	20	20
4	Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине	*Диф.зачёт* -		
5	**Трудоёмкость дисциплины Всего: в часах (ч) в зачётных единицах (ЗЕ)**	-	**144 / 4**	**144/ 4**

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 и виды занятий (очная форма обучения)							Трудоёмкость, ч / ЗЕ
			аудиторная работа					Итоговый контроль	самостоятельная работа	
			всего	Л	ПЗ	ЛР	КСР			
1	1	1	9	1	8				6	**15**
		2	12	2	8	-	2		6	**18**
		3	10	2	8	-			6	**16**
		4	10	2	8				6	**16**
	Всего по модулю:		**41**	**7**	**32**	**-**	2		**24**	**65**
		5	9	1	8				6	**15**
		6	10	2	8				6	**16**
		7	9	1	8				6	**15**
		8	10	2	8				6	**16**
		9	11	1	8		2		6	**17**
	Всего по модулю:		**49**	**7**	**40**	**-**	**2**		**30**	**79**
Промежуточная аттестация										
Итого:			**90**	**14**	**72**	**-**	**4**		**54**	**144/4ЗЕ**

4.2. Содержание разделов и тем учебной дисциплины

Модуль 1. Информационная безопасность кадровой работы

Раздел 1. Информационная безопасность кадровой работы

Л – 7 ч, ПЗ – 32 ч, ЛР - нет, КСР – 2, СРС –24

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 информации

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

Тема 2. Угрозы конфиденциальной информации и системы ее защиты

Риски угроз информационной безопасности. 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.

Модуль 2. Информационная безопасность коммерческой деятельности

Раздел 2. Л – 7 ч, ПЗ – 40 ч, ЛР - нет, КСР – 2 ч., СРС – 30 ч.

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.

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.

Тема 9. Аудит системы информационной безопасности

Аудит системы управления информационной безопасности. Этапы проведения аудита. Политика информационной безопасности. Разделы политики

4.3. Перечень тем практических занятий

Таблица 4.3 – 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
2	2	Выявление угроз и уязвимостей информационной безопасности. Определение мер для снижения рисков угроз информационной безопасности
3	3	Составление перечня конфиденциальных документов. Разработка разрешительной системы допуска к конфиденциальным документам.
4	4	Выявление угроз безопасности, реализуемые через персонал. Разработка процедур работы с конфиденциальными документами. Групповая работа над проектом
5	5	Угрозы и уязвимости конфиденциального документооборота на цифровых носителях. Разрешительная система допуска сотрудников к конфиденциальным документам
6	6	Документооборот на цифровых носителях. Меры защиты в отношении цифровых документов.
7	7	Определение перечня потенциально возможных угроз интересам предприятия. Определение возможного ущерба, который может возникнуть в результате реализации подобных угроз
8	8, 9	Проведение аудита системы управления информационной безопасности. Политика информационной безопасности.

4.4. Перечень тем лабораторных работ

Не предусмотрены

5. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимися целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику, конспектным материалам или по материалам страницы дисциплины на портале рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, и индивидуальным комплексным заданиям на самостоятельную работу.
4. Изучение дисциплины осуществляется в течение одного семестра, график изучения дисциплины приводится п.7.
5. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

5.1. Виды самостоятельной работы студентов

Таблица 5.1 – Виды самостоятельной работы студентов (СРС)

Номер темы (раздела) 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*	6
3	*Подготовка к практическим занятиям:* - Риски информационной безопасности. Основные подходы к управлению рисками. - Стратегия управления рисками разных классов конфиденциальности.	3
4	*Подготовка к практическим занятиям:* - Сущность и особенности конфиденциального документооборота. Особенности и задачи конфиденциального делопроизводства. - Организация конфиденциального делопроизводства. Подготовка и издание конфиденциальных документов. - Организация конфиденциального документооборота.	3

	Формирование и оформление конфиденциальных дел	
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.	4
6	*Подготовка к практическим занятиям:* Особенности документооборота на цифровых носителях. Меры защиты в отношении цифровых документов. Процедуры контроля использования мобильных носителей информации. Процедуры контроля использования ресурсов Интернета	3
7	*Подготовка к практическим занятиям:* Определение перечня потенциально возможных угроз интересам предприятия. Определение возможного ущерба, который может возникнуть в результате реализации подобных угроз	4
8	*Подготовка к практическим занятиям:* Аудит системы управления информационной безопасности. Политика информационной безопасности.	3
9	*Выполнение индивдуальных заданий*	20
	Итого: в **ч** / в **ЗЕ**	54/1,5

5.2. Индивидуальные задания

Индивидуальные задания являются комплексными, охватывают все темы дисциплины и выполняются в форме документов с ссылками на созданные ресурсы согласно теме, выданной преподавателем. Список типовых заданий:

Темы заданий:

1. Для конкретной (условной) компании
    a. Определить перечень сведений, относимых к коммерческой тайне.
    b. Составить перечень документов по классам конфиденциальности.

2. Для конкретной (условной) компании
    a. Выявить угрозы и уязвимости информационной безопасности.
    b. Определить меры для снижения рисков угроз информационной безопасности.
3. Для конкретной (условной) компании
    a. Составить перечень конфиденциальных документов.

b. Определить угрозы и уязвимости конфиденциального документооборота

4. Для конкретной (условной) компании
   a. Разработать разрешительную систему допуска сотрудников к конфиденциальным документам
5. Для конкретной (условной) компании
   a. Выявить угрозы безопасности, реализуемые через персонал.
   b. Разработать процедуру работы с конфиденциальными документами
6. Для конкретной (условной) компании
   a. Разработать процедуру подбора персонала, имеющих доступ к конфиденциальной информации
   b. Разработать процедуру работы с документами по приему сотрудников

5.3. Образовательные технологии, используемые для формирования компетенций

Лекционные занятия проводятся с использованием презентаций. В процессе лекций постоянно проводится опрос по ранее пройденному материалу. Материалы лекций опубликованы на странице дисциплины на портале гуманитарного факультета[1] и включают, в том числе видеолекции.

Практические занятия проводятся в аудитории. При проведении практических занятий преследуются следующие цели:

- изучение законов и положений в области информационной безопасности;
- закрепление навыков по выявлению угроз информационной безопасности;
- отработка навыков по выявлению информационных ресурсов и распределению их по степени конфиденциальности

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 контроль освоения заданных дисциплинарных частей компетенций проводится в виде теоретических опросов на лекции. Теоретический опрос студентов проводится по каждому разделу. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя, и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

6.2. Рубежный контроль освоения заданных частей дисциплинарных компетенций

Рубежный контроль освоения дисциплинарных компетенций проводится в форме выполнения индивидуальных и практических заданий

6.3. Итоговый контроль освоения заданных частей дисциплинарных компетенций

Допуск к дифференцированному зачету осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача результатов всех практи-

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

ческих и индивидуальных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Аттестация, согласно РПД, проводится в виде зачета по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний. Умения и владения оцениваются в ходе рубежного и промежуточного контроля.

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

Таблица 6.1 - Виды контроля освоения элементов и частей компетенций

Контролируемые результаты освоения дисциплины (ЗУВы)	**Вид контроля**		
	Текущий	Рубежный	Диф-зач
Знает			
-З1 Основные угрозы информационной безопасности предприятия и их источники	ТО		ТВ
-З2 Классы информационных ресурсов по степени конфиденциальности	ТО		ТВ
- З3Угрозы и защита безопасности со стороны персонала	ТО		
Умеет			
- У1 Использовать необходимые действия для уменьшения рисков и угроз информационной безопасности.		ПЗ	
-У2 Организовать защиту персональных данных сотрудников.		ПЗ	
- У3 Организовать архивное хранение кадровых документов.		ПЗ	
Владеет			
- В1 Современными технологиями для организации защиты информационных ресурсов предприятия.		ИЗ	
-В2 навыками работы с конфиденциальной информацией		ИЗ	

ТО – теоретический опрос по теме;
ИЗ – индивидуальные задания;
ПЗ – практические задания;
ТВ – теоретический вопрос

Фонды оценочных средств, включающие индивидуальные и практические задания, контрольные вопросы входят в состав РПД в виде отдельного приложения.

7 График учебного процесса по дисциплине

Таблица 7.1 – График учебного процесса по дисциплине

Вид работы	**Распределение 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**		**1**		**1**		**1**		**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**		**14**
Практические занятия	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**72**
Семинары																			
Лабораторные работы																			**-**
КСР		**2**																**2**	**4**
Подготовка к занятиям	2	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	2	**36**
Самостоятельное изучение теоретического материала	**-**	**1**	**1**	**1**		**1**	**1**		**1**	**1**	**1**	**1**	**1**	**1**	**1**		**1**	**1**	**14**
Индивидуальное задание (реферат)	2	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**20**
	10	**10**	**9**	**8**	**8**	**8**	**9**	**7**	**9**	**9**	**10**	**9**	**9**	**9**	**9**	**8**	**9**	**10**	**144**
Модуль:	**М1**		**М2**																
Контр. тестирование																			
Дисциплин. контроль																			**Диф/Зачёт**

8 Учебно-методическое и информационное обеспечение дисциплины

8.1 Карта обеспеченности дисциплины учебно-методической литературой

Б1.В.02 Информационная безопасность в кадровой работе	**Блок 1** (*цикл дисциплины*)
(*полное название дисциплины*)	[x] обязательная; [ ] по выбору студента; [ ] базовая часть цикла; [×] вариативная часть цикла

38.03.03	***Управление персоналом/Управление персоналом организации***
(*код направления / специальности*)	(*полное название направления подготовки / специальности*)

УП/УПО	Уровень подготовки	Форма обучения
(*аббревиатура направления / специальности*)	[ ] специалист; [×] бакалавр; [ ] магистр	[×] очная; [ ] заочная; [ ] очно-заочная

2016
Год утверждения уч.плана ОПОП

Семестр(ы) 8

Количество групп 1

Количество студентов 20

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.	*6 +ЭБ*
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 **Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**		
	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	

Основные данные об обеспеченности на ___ 21.05.2017 _____
(*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 _____
(*дата контроля литературы*)

Основная литература	[ ]	обеспечена	[ ]	не обеспечена
Дополнительная литература	[ ]	обеспечена	[ ]	не обеспечена

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

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 8.2 – 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	Сервисы Web 2.0		Создание контента с использованием облачных сервисов. Публикация и настройки совместного доступа

8.4. Аудио- и видео-пособия

Таблица 8.3 – Используемые аудио- и видео-пособия

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

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		