УОП 37

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
Пермский национальный исследовательский политехнический университет

Гуманитарный факультет

Кафедра «Менеджмент и маркетинг»

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

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Информационная безопасность»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программа академического бакалавриата

Направление **09.03.03** «Прикладная информатика»

Профиль программы бакалавриата **«Прикладная информатика в экономике»**

Квалификация выпускника: **Бакалавр**

Выпускающая кафедра: **«Менеджмент и маркетинг»**

Форма обучения: **заочная**

Курс: 3 **Семестр**: 5

Трудоёмкость:
Кредитов по рабочему учебному плану: 5 ЗЕ
Часов по рабочему учебному плану: 180 ч

Виды контроля:
Экзамен: 5 семестр Контрольная работа: 5 семестр

Пермь
2016

Учебно-методический комплекс дисциплины Б1.В.02 Информационная безопасность разработан на основании:

- федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки Российской Федерации «12» марта 2015 г. номер Государственной регистрации «207» по направлению **09.03.03 «Прикладная информатика»;**
- компетентностной модели выпускника ОПОП по направлению **09.03.03 «Прикладная информатика»** и профилю подготовки «Прикладная информатика в экономике», утверждённой «24» июня 2013 г. (с изменениями в связи с переходом на ФГОС ВО);
- учебного плана заочной формы обучения, по направлению **09.03.03 «Прикладная информатика»** и профилю подготовки «Прикладная информатика в экономике», утверждённого «28» апреля 2016 г.

Рабочая программа согласована с рабочими программами дисциплин Логистика, Информационные системы и технологии, Системная архитектура информационных систем, Управление информационными ресурсами, Экономические информационные системы, Информационные системы в менеджменте, Программная инженерия, Интеллектуальные информационные системы, Бюджетирование.

Разработчик: ст. преподаватель С.М. Королев

Рецензент: канд. техн. наук, доц. С.И. Косякин

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

Заведующий кафедрой,
менеджмента и маркетинга
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 социол. наук, проф. В.Н. Стегний

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

1 Общие положения

1.1 Цель учебной дисциплины - формирование комплекса знаний, умений и навыков в области информационной безопасности; источников рисков и форм атак на информацию; угроз, которым подвергается информация; вредоносных программам; защиты от компьютерных вирусов и других вредоносных программам; методов и средств защиты информации; политик безопасности компании в области информационной безопасности; стандартов информационной безопасности; криптографических методов и алгоритмов шифрования информации; алгоритмов аутентификации пользователей; защиты информации в сетях; требований к системам защиты информации.

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

- способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе (ПК-1);
- способность документировать процессы создания информационных систем на стадиях жизненного цикла (ПК-4);
- способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (ПК-18).

1.2 Задачи дисциплины:

- Изучение теории безопасности информационных систем;
- Изучение тенденций развития защиты информационной с моделями возможных угроз,
- Изучение терминологии и основных понятий в области защиты информации;
- Изучение международных стандартов информационного обмена;
- Изучение понятия вредоносных программ;
- Изучение руководящих документов в области защиты информации;
- Изучение методов криптографии.
- Формирование умения проводить аудит защищенности сети с использованием сетевого сканера;
- Формирование навыков использования цифровых сертификатов для формирования электронно-цифровой подписи, шифрования информации, настройка аутентификации пользователей;
- Формирование навыков использования криптографических алгоритмов, а также противодействия несанкционированного доступа.

1.3 Предметом освоения дисциплины являются следующие объекты:

- Информационная безопасность.
- Методы криптографии.

- Методы защиты информационных систем от несанкционированного проникновения.
- Методы исследования и анализ причин нарушения безопасности компьютерных систем.

1.4 Место учебной дисциплины в структуре образовательной программы.

Дисциплина **Б1.В.02 Информационная безопасность** относится к *вариативной* части блока 1 Дисциплины (модули) и является *обязательной дисциплиной* при освоении ОПОП по *профилю* «Прикладная информатика в экономике».

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

знать:

- понятия информационной безопасности в условиях функционирования в России глобальных сетей;
- три вида возможных нарушений информационной системы;
- необходимые положения Конституции и ГК РФ для формирования политик информационной безопасности;
- понятия вредоносных программ;

уметь:

- выполнять исследование ИС на предмет несанкционированного проникновения;
- выполнять анализ рисков в соответствии с требованиями стандарта ИСО/МЭК 17799;
- выполнять аудит защищенности сети с использованием сетевого сканера;
- создавать регламентирующие документы и стандарты в области управления информационной безопасностью;
- составлять многоуровневую защиту корпоративных сетей;
- выполнять установку программных и аппаратных средств защиты информационных систем;

владеть:

- навыками использования криптографических моделей, алгоритмов шифрования информации и аутентификации пользователей;
- навыками формирования политик в области управления информационной безопасностью.
- навыками использования цифровых сертификатов для формирования электронно-цифровой подписи;
- навыками использования программных средств для защиты от вредоносных программ.

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

Код	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Профессиональные компетенции			
ПК-1	способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе	Логистика, Информационные системы и технологии, Системная архитектура информационных систем	Управление информационными ресурсами, Экономические информационные системы, Информационные системы в менеджменте
ПК-4	способность документировать процессы создания информационных систем на стадиях жизненного цикла	Информационные системы и технологии	Программная инженерия, Интеллектуальные информационные системы
ПК-18	способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	Бюджетирование	Управление информационными ресурсами

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

Учебная дисциплина обеспечивает формирование части компетенций ПК-1 и ПК-4, ПК-18.

2.1 Дисциплинарная карта компетенции ПК-1

Код ПК-1	**Формулировка компетенции:** способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе
Код ПК-1.Б1.В.02	**Формулировка дисциплинарной части компетенции:** способность проводить обследование организаций и формировать требования к системе информационной безопасности

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции студент: **Знает:** - понятия информационной безопасности в условиях функционирования в России глобальных сетей; - три вида возможных нарушений информационной системы; **Умеет:** - выполнять исследование ИС на предмет несанкционированного проникновения; - выполнять анализ рисков в соответствии с требованиями стандарта ИСО/МЭК 17799; - выполнять аудит защищенности сети с использованием сетевого сканера; **Владеет:** - навыками использования криптографических моделей, алгоритмов шифрования информации и аутентификации пользователей.	Лекции. Самостоятельная работа студентов по изучению теоретического материала. Практические занятия. Самостоятельная работа по подготовке к практическим занятиям. Практические занятия.	Вопросы текущего контроля. Вопросы к экзамену. Отчет по практическим заданиям. Вопросы к экзамену. Задания к практическим занятиям. Вопросы к экзамену.

2.2 Дисциплинарная карта компетенции ПК-4

Код ПК-4	**Формулировка компетенции:** способность документировать процессы создания информационных систем на стадиях жизненного цикла
Код ПК-4.Б1.В.02	**Формулировка дисциплинарной части компетенции:** способность документировать процессы создания системы информационной безопасности

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки

Знает: - необходимые положения Конституции и ГК РФ для формирования политик информационной безопасности; **Умеет:** - создавать регламентирующие документы и стандарты в области управления информационной безопасностью; **Владеет:** - навыками формирования политик в области управления информационной безопасностью. - навыками использования цифровых сертификатов для формирования электронно-цифровой подписи.	Лекции. Самостоятельная работа студентов по изучению теоретического материала. Практические занятия. Самостоятельная работа по подготовке к практическим занятиям. Практические занятия. Самостоятельная работа по подготовке к экзамену.	Вопросы текущего контроля. Вопросы к экзамену. Отчет по практическим заданиям. Вопросы к экзамену. Задания к практическим занятиям. Вопросы к экзамену.

2.3 Дисциплинарная карта компетенции ПК-18

Код ПК-18	**Формулировка компетенции:** способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью
Код ПК-18.Б1.В.02	**Формулировка дисциплинарной части компетенции:** способность принимать участие в управлении информационной безопасностью

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции студент: **Знает:** - понятия вредоносных программ; **Умеет:** - составлять многоуровневую защиту корпоративных сетей; - выполнять установку программных и аппаратных средств защиты информационных систем; **Владеет:** - навыками использования программных средств для защиты от вредоносных программ.	Лекции. Самостоятельная работа студентов по изучению теоретического материала. Практические занятия. Самостоятельная работа по подготовке к практическим занятиям. Практические занятия.	Вопросы текущего и рубежного контроля. Вопросы к экзамену. Отчет по практическим заданиям. Задания к практическим занятиям.

3 Структура учебной дисциплины по видам и формам учебной работы

Объем дисциплины в зачетных единицах составляет 5 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, ч	
		по семестрам	всего
1	2	3	5
1	**Аудиторная (контактная работа)**	20	**20**
	- лекции (Л)	8	**8**
	- практические занятия (ПЗ)	10	**10**
	- контроль самостоятельной работы (КСР)	2	**2**
2	**Самостоятельная работа студентов** (СРС)	151	**151**
	- изучение теоретического материала	80	**80**
	- подготовка к практическим занятиям	32	**32**
	- подготовка отчета по практическим занятиям	29	**29**
	- выполнение контрольной работы	10	**10**
3	Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине:	экзамен	**9**
4	**Трудоёмкость дисциплины, всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	**180**	**180** **5**

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 (заочная форма обучения)							Трудоёмкость, ч / ЗЕ
			аудиторная работа					итоговый контроль	самостоятельная работа	
			всего	Л	ПЗ	ЛР	КСР			
1	2	3	4	5	6	7	8	9	10	11
1	1	1	2	1	1				14	16
		2	2	1	1				18	20
		3	2	1	1				18	20
		4	3	1	1		1		18	20
	Итого по модулю:		**9**	**4**	**4**		**1**		**68**	**77**
2	2	5	2	1	1				18	20
		6	2	1	1				18	20
		7	3	1	2				18	20
		8	4	1	2		1		19	23
	Итого по модулю:		**11**	**4**	**6**		**1**		**73**	**84**
Контрольная работа									**10**	**10**
Промежуточная аттестация								**9**		**9**
Всего:			**20**	**8**	**10**		**2**	**9**	**151**	**180/5**

4.2 Содержание разделов и тем учебной дисциплины

Модуль 1. Базовые понятия информационной безопасности
Раздел 1. Базовые понятия информационной безопасности
Л - 4 ч., ПЗ – 4 ч., СРС – 68 ч., КСР – 1 ч.

Тема 1. Базовые понятия. Международные стандарты информационного обмена. Понятие угрозы. Исследование информационных систем на предмет не санкционированного проникновения.

Тема 2. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников (нарушителей). Понятие о видах вирусов. Анализ рисков в соответствии с требованиями стандарта ИСО/МЭК 17799.

Тема 3. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Аудит защищенности сети с использованием сетевого сканера.

Тема 4. Понятия вредоносных программ. Виды нарушений информационной безопасности. Защита информации и информационная безопасность. Руководящие документы области защиты информации. Использование программных средств для защиты от вредоносных программ.

Модуль 2. Принципы построения защищенных ИС
Раздел 2. Принципы построения защищенных ИС
Л - 4 ч., ПЗ – 6 ч., СРС – 73 ч., КСР – 1 ч.

Тема 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Основные положения теории безопасности информационных систем. Разработка стандартов и регламентов информационной безопасности.

Тема 6. Модели безопасности и их применение. Виды разведок и противодействия разведке. Анализ способов нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Методы криптографии. Использование криптографических методов для шифрования данных.

Тема 7. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Установка программных и аппаратных средств защиты информационных систем.

Тема 8. Использование защищенных компьютерных систем. Основные технологии построения защищенных ЭИС. Концепция информационной безопасности. Практическое использование цифровых сертификатов для формирования электронно-цифровой подписи, шифрования информации, надежной аутентификации пользователей. Место информационной безопасности экономических систем в национальной безопасности страны.

4.3 Перечень тем практических занятий

Таблица 4.2 – Темы практических занятий

№ п/п	Номер темы дисциплины	Наименование темы практического занятия
1	**2**	**3**
1	Тема 1	Исследование информационных систем на предмет не санкционированного проникновения.
2	Тема 2	Анализ рисков в соответствии с требованиями стандарта ИСО/МЭК 17799.
3	Тема 3	Аудит защищенности сети с использованием сетевого сканера.
4	Тема 4	Использование программных средств для защиты от вредоносных программ.
5	Тема 5	Разработка стандартов и регламентов информационной безопасности.
6	Тема 6	Использование криптографических методов для шифрования данных.
7	Тема 7	Установка программных и аппаратных средств защиты информационных систем.
8	Тема 8	Практическое использование цифровых сертификатов для формирования электронно-цифровой подписи, шифрования информации, надежной аутентификации пользователей.

4.4 Лабораторные работы
Лабораторные работы не предусмотрены.

4.5 Курсовой проект (курсовая работа)
Курсовой проект не предусмотрен.

4.6 Реферат
Реферат не предусмотрен.

4.7 Расчетно-графические работы
Расчетно-графические работы не предусмотрены.

5 Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам 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)

№ темы дисциплины	Вид самостоятельной работы студентов	Трудоёмкость, час.
Тема 1	**Изучение теоретического материала.** Понятия рисков и методы их анализа.	10
	Подготовка к практическим занятиям. Основные правила исследования информационных систем на предмет не санкционированного проникновения.	4
Тема 2	**Изучение теоретического материала.** Изучить понятие программы – вируса.	10
	Подготовка к практическим занятиям. Требования стандарта ИСО/МЭК 17799.	4
	Подготовка отчёта по практическим занятиям.	4
Тема 3	**Изучение теоретического материала.** Изучить нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы в области информационной безопасности.	10
	Подготовка к практическим занятиям. Назначение сетевого сканера.	4
	Подготовка отчёта по практическим занятиям.	4
Тема 4	**Изучение теоретического материала**. Изучить понятие вредоносной программы.	10
	Подготовка к практическим занятиям. Виды вредоносных программ.	4
	Подготовка отчёта по практическим занятиям.	4
Тема 5	**Изучение теоретического материала.** Какие задачи в сфере обеспечения информационной безопасности преследует государство?	10
	Подготовка к практическим занятиям. Правила разработки стандартов и регламентов информационной безопасности.	4
	Подготовка отчёта по практическим занятиям.	4
Тема 6	**Изучение теоретического материала.** Изучить виды разведок и противодействия разведке.	10
	Подготовка к практическим занятиям. Методы криптографии.	4

	Подготовка отчёта по практическим занятиям.	4
Тема 7	**Изучение теоретического материала.** Изучить понятие таксономия нарушений информационной безопасности.	10
	Подготовка к практическим занятиям. Виды программных и аппаратных средств защиты информационных систем.	4
	Подготовка отчёта по практическим занятиям.	4
Тема 8	**Изучение теоретического материала.** Изучить место информационной безопасности экономических систем в национальной безопасности страны.	10
	Подготовка к практическим занятиям. Использование цифровых сертификатов для формирования электронно-цифровой подписи.	4
	Подготовка отчёта по практическим занятиям.	5
	Выполнение контрольной работы.	**10**
	Итого: в **ч** / в **ЗЕ**	**151** **4,19**

5.2 Контрольная работа

Тематика контрольных работ:

Провести анализ угроз и предложить способы защиты в области информационной безопасности конкретного предприятия.

Указания по подготовке контрольной работы.

Для подготовки контрольной работы преподаватель на занятии выдает студенту описание предприятия из представленного перечня. Студент может взять в качестве исследуемого объекта предприятие, на котором он работает, по согласованию с преподавателем. Контрольная работа выполняется самостоятельно **в соответствии с Методическими рекомендациями по самостоятельной работе**.

5.3 Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. Обучающиеся взаимодействуют не только с преподавателем, но и друг с другом. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем; отработка у обучающихся навыков взаимодействия в составе проектной группы; закрепление основ теоретических знаний.

6 Фонд оценочных средств дисциплины

6.1 Текущий контроль освоения заданных дисциплинарных частей компетенций

Текущий контроль освоения дисциплинарных компетенций проводится в следующих формах:

- контроль теоретического материала проводится на основании опроса и умения применить теоретический материал на практических заданиях.

6.2 Рубежный контроль освоения заданных дисциплинарных частей компетенций

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

- защиты отчетов по практическим занятиям;
- контрольная работа.

6.3 Итоговый контроль освоения заданных дисциплинарных частей компетенций (промежуточная аттестация)

Экзамен

Экзамен по дисциплине проводится в устной форме с использованием фонда оценочных средств (билетам) по дисциплине (разрабатывается отдельным документом).

Выполненная контрольная работа является допуском до экзамена.

Экзаменационная оценка выставляется с учетом результатов промежуточного контроля.

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

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 обучения по дисциплине (ЗУВы)		Вид контроля			
		Текущий		Рубежный	Промежуточная аттестация
		ТТ	ОПЗ	ИЗ	Экзамен
1		2	3		5
знает					
З1	понятия информационной безопасности в условиях функционирования в России глобальных сетей				ТВ
З2	три вида возможных нарушений информационной системы				ТВ

З3	необходимые положения Конституции и ГК РФ для формирования политик информационной безопасности				ТВ
З4	понятия вредоносных программ				ТВ
умеет					
У1	выполнять исследование ИС на предмет несанкционированного проникновения		ОПЗ.1		ТВ
У2	выполнять анализ рисков в соответствии с требованиями стандарта ИСО/МЭК 17799		ОПЗ.1		ТВ
У3	выполнять аудит защищенности сети с использованием сетевого сканера		ОПЗ.1		ТВ
У4	создавать регламентирующие документы и стандарты в области управления информационной безопасностью		ОПЗ.2		ТВ
У5	составлять многоуровневую защиту корпоративных сетей		ОПЗ.3		ТВ
У6	выполнять установку программных и аппаратных средств защиты информационных систем		ОПЗ.3		ТВ
владеет					
В1	навыками использования криптографических моделей, алгоритмов шифрования информации и аутентификации пользователей			ИЗ.1	ТВ
В2	навыками формирования политик в области управления информационной безопасностью			ИЗ.1	ТВ
В3	навыками использования цифровых сертификатов для формирования электронно-цифровой подписи			ИЗ.1	ТВ
В4	навыками использования программных средств для защиты от вредоносных программ			ИЗ.1	ТВ

Условные обозначения:

ТО – теоретический опрос;
ОПЗ – отчет о практическом занятии;
ИЗ – индивидуальное задание;
ТВ – теоретический вопрос.

7 График учебного процесса по дисциплине

Таблица 7.1 – График учебного процесса по дисциплине (5-й семестр)

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**	**19**	**20**	
Лекции	4	4	2																		**8**
Практические занятия	2	4	4																		**10**
Самостоятельное изучение теоретического материала	10	10	10		10		10		10		10		10								**80**
Подготовка к практическим занятиям	10	10	12																		**32**
Подготовка отчёта по практическим занятиям	4	4	4			4		4		4		4		1							**29**
Выполнение контрольной работы																	5		5		**10**
Представление контрольной работы (КСР)																				2	**2**
Дисциплин. контроль																				9	**Экзамен**

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

8.1 Карта обеспеченности дисциплины учебно-методической литературой

Б1.В.02 Информационная безопасность	Блок 1. Дисциплины (модули)
	[x] обязательная / [ ] по выбору студента; [ ] базовая часть цикла / [x] вариативная часть цикла
09.03.03	Направление «Прикладная информатика», профиль «Прикладная информатика в экономике»

ПИФ/ИЭ
(*аббревиатура направления / специальности*)

Уровень подготовки: [ ] специалист [x] бакалавр [ ] магистр

Форма обучения: [ ] очная [x] заочная [ ] очно-заочная

2016
(*год утверждения учебного плана ОПОП*)

Семестр: 5

Количество групп 1

Количество студентов 25

Королев С.М. ст.преподаватель

Гуманитарный

Менеджмента и маркетинга 89223121111, 241-41-50

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 и защита информации : учебное пособие для вузов / Ю. Ю. Громов [и др.] .— 2-е изд., перераб. и доп .— Старый Оскол : ТНТ, 2016 .— 383 с., 22,32 усл. печ. л. : ил.	2010 -5 2016 - 2
2.	Ахметова, Светлана Геннадьевна. Информационная безопасность [Электронный ресурс] : электронное мультимедийное пособие / С. Г. Ахметова ; Пермский национальный исследовательский политехнический университет .— Электрон. дан. и прогр. (24,8 Мб) .— Пермь : Изд-во ПНИПУ, 2013 .— 1 электрон. опт. диск (CD-ROM)	1+ЭБ
3.	Ахметова, Светлана Геннадьевна. Информационная безопасность : учебно-методическое пособие / С. Г. Ахметова ; Пермский национальный исследовательский политехнический университет .— Пермь : Изд-во ПНИПУ, 2013 .— 122 с., 7,75 усл. печ. л. : ил.	6+ЭБ
2 Дополнительная литература		
2.1 Учебные и научные издания		
4.	Глинская, Елена Вячеславовна. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е. В. Глинская, Н. В. Чичварин .— Москва : ИНФРА-М, 2016 .— 117 с., 7,37 усл. печ. л. : ил .	2
5.	Бабаш, А. В. Информационная безопасность. История защиты информации в России : учебное пособие / А. В. Бабаш, Е. К. Баранова, Д. А. Ларин .— Москва : Университет, 2015 .— 736 с., 42,78 усл. печ. л. : ил.	2
6.	Мельников, Дмитрий Анатольевич. Информационная безопасность открытых систем : учебник / Д. А. Мельников .— Москва : Флинта : Наука, 2013 .— 442 с., 27,44 усл. печ. л. : ил. — Список сокр.: с. 433-435 .	11
2.2 Периодические издания		
	Не предусмотрены	
2.3 Нормативно-технические издания		
	Не предусмотрены	
2.4 Официальные издания		
	Не предусмотрены	
2.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины		
1.	**Электронная библиотека** Научной библиотеки Пермского национального исследовательского политехнического университета [Электронный ресурс : полнотекстовая база данных электрон. документов изданных в Изд-ве ПНИПУ]. – Электрон. дан. (1 912 записей). – Пермь, 2014- . – Режим доступа: http://elib.pstu.ru/. – Загл. с экрана.	

Основные данные об обеспеченности на _____

Основная литература [x] обеспечена [ ] не обеспечена

Дополнительная литература [x] 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

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

Не предусмотрены

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	
1	2	3	4	5
		+		Курс лекций

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	2	3	4	5	6
1	Мультимедиа класс	Кафедра МиМ	506 к.А	50	50

9.2 Основное учебное оборудование

Не предусмотрено